

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Quelques considérations sur le droit du cyberspace

Poullet, Yves

Published in:

Les dimensions internationales du droit du cyberspace

Publication date:

2000

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Poullet, Y 2000, Quelques considérations sur le droit du cyberspace. Dans *Les dimensions internationales du droit du cyberspace*. Droit du Cyberspace, Editions UNESCO , Paris, p. 185-235.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Quelques considérations sur le droit du cyberspace ¹

Yves POULLET

« On souligne l'ardente obligation de l'État d'intervenir au moment où, selon nous, délaisser l'Internet et se retirer de sa réglementation à tel point qu'il n'en fixe même plus le cadre général, parce que, notamment, l'ordre public, les libertés fondamentales et d'autres valeurs de base sont en jeu. » ²

INTRODUCTION

« Au fur et à mesure que le cyberspace devient un milieu de vie, s'accroît l'importance d'y trouver des règles du jeu adaptées et équilibrées. » ³ Ces règles sont-elles nouvelles ? Grande est la tradition d'affirmer qu'à la révolution de l'Internet doit correspondre une révolution du droit. Comme le note le document de travail de la réunion d'experts sur le droit du cyberspace organisée par l'UNESCO en septembre 1998 à Monte-Carlo, intitulée *Info-éthique* ⁴ : « La doctrine juridique la plus autorisée convient que la révolution occasionnée par l'Internet d'aujourd'hui et qui sera confirmée par la société de l'information de demain, doit correspondre en tout état de cause à une révolution du Droit au sens large du terme. »

1. Les réflexions présentées dans ce texte ont été soumises le 20 mars 1998, au groupe « Société de l'information » réuni par l'Académie royale belge des sciences. Cet article a été rédigé dans le cadre des recherches menées au nom du programme « Pôles d'attraction interuniversitaire pour le compte de l'État belge », services du Premier Ministre et services fédéraux des affaires scientifiques, techniques et culturelles.

2. Y. Poulet, « Quelques considérations dans le droit du cyberspace », § 2.2.3.

3. P. Trudel, 1997.

4. UNESCO, Réunion d'experts sur le droit du cyberspace, (Doc. CII-98/CONF-601.2, § 12).

Le cyberspace se caractérise des deux manières suivantes :

- Premièrement, le cyberspace ignore les frontières, or le droit s'appuie d'abord et avant tout sur un État territorial capable de maîtriser des situations localisées sur son territoire. « Le cyberspace comporte une remise en cause des frontières qu'il ignore et du droit étatique qu'il défie. »⁵

- Deuxièmement, le cyberspace est un espace jamais clos, toujours redéfini à la faveur des hyperliens que les utilisateurs activent. À la faveur de ces possibilités infinies, s'effondrent les distinctions par lesquelles le droit appréhendait la régulation de la communication⁶ : celle des acteurs, au moment où n'importe qui peut être producteur d'informations, intermédiaires ou consommateurs de celles-ci ; la distinction réglementaire traditionnelle entre les médias qui cloisonnait le droit de la presse, de l'audiovisuel et des télécommunications et ce au moment où écrit, texte et sons se mêlent ; l'opposition classique du droit des produits, d'une part et du droit des services, d'autre part, à l'heure où la digitalisation totale des « produits informationnels » rend cette distinction malaisée. Ensuite, la notion d'œuvre n'est plus nécessairement liée à une personne et à un support mais plutôt à un objet, voire à un processus où nombre d'individus peuvent coopérer. Enfin, les frontières entre communications publiques et communications privées s'estompent.

Ainsi disparaissent à la fois, dans notre « village global », le lieu « naturel » d'intervention du droit et les structures ou concepts par lesquels ce dernier opérait traditionnellement⁷.

Nous tenterons à partir de ce constat quelques réflexions qui inspireront notre propos :

- Il faudra tout d'abord rendre attentif le juriste au fait que non seulement le développement des technologies de l'information et de la communication demande à ce que les concepts traditionnels soient approfondis, mais plus encore, que souvent il modifie les équilibres inscrits au cœur des réglementations et exige alors des interventions nouvelles du droit (Partie I).

- Ensuite, je m'interrogerai sur les nouveaux modes de productions du droit. Grande est en effet la tentation d'abandonner à l'autorégulation et à la technique la tâche de régler les comportements sociaux dans le cyberspace. Dans cette perspective, je ques-

tionnerai le rôle du droit étatique et le dialogue possible entre les normativités réglementaires, techniques et les nombreuses manifestations de l'autorégulation (Partie II).

- Enfin, j'analyserai les valeurs que le droit se doit de promouvoir pour que notre société ne soit pas seulement informationnelle mais également démocratique (Partie III).

1. UN DROIT QUI BOUSCULE : DE L'APPROFONDISSEMENT DES CONCEPTS À L'ÉLARGISSEMENT DES DÉBATS

Digitalisée, véhiculée par des réseaux couvrant la terre entière, objet de multiples traitements, traduite en de multiples supports, l'information se révèle insaisissable... aux yeux du droit également. Dans ce cadre éclatent les cloisonnements traditionnels, base de nos réglementations. Cet éclatement a tout à la fois une dimension géographique, professionnelle et disciplinaire. À cet éclatement, s'oppose le devoir de retenue du juriste, c'est-à-dire, d'une part, l'obligation qui lui est faite de confronter la nouveauté aux concepts anciens et aux valeurs que ces concepts traduisent et, d'autre part, l'obligation de ne s'en écarter que lorsque l'analyse révèle, de façon patente, l'impossibilité de s'en satisfaire ou la nécessité de protéger des valeurs nouvelles.⁸

Notre propos s'éclaire de considérations tirées de deux débats récents :

- le premier concerne celui de la signature électronique ;
- le deuxième s'attache aux conséquences des systèmes de gestion électronique des droits d'auteur, les dits « ECMS » (Electronic Copyright Management Systems), selon la terminologie anglaise couramment utilisée.

Les conclusions tirées à partir de ces deux exemples mettront en évidence quelques réflexions sur le couple Droit-Technologie.

1.1. La signature sous toutes ses formes

Approfondir le droit : une approche fonctionnelle de la signature

Le problème de la validité de la signature électronique semble, suite aux travaux de la Commission des Nations Unies pour le droit

5. UNESCO, *op. cit.*, § 10.

6. P. Poulet, 1993 ; J. Reidenberg, 1996.

7. C. Lamouline et Y. Poulet, 1997.

8. S. Gutwirth, 1993.

commercial international (CNUDCI)⁹ ou à la proposition de directive 98/297/UE relative à un cadre commun en matière de signature électronique, avoir été résolu par une approche fonctionnelle de celle-ci. Faut-il modifier profondément notre législation du droit de la preuve pour y faire entrer la réalité des ordinateurs et des technologies de la communication ? Non. L'ouverture « providentielle » du concept juridique de signature permet d'accueillir la réalité nouvelle en exigeant des modes techniques de création et d'apposition de signature, les mêmes exigences fonctionnelles que celles de la signature manuscrite : l'identification du signataire, l'authentification d'un document auquel sa signature doit rester attachée. Ainsi, et on le constate bien souvent, le développement des technologies de l'information et de la communication sont l'occasion de revitaliser les concepts traditionnels. Il convient de souligner le danger de solutions *ad hoc* qui, si elles ont l'avantage de la simplicité apparente, créent à terme des perturbations graves dans l'ordre juridique.

Dans le passé, les tentatives de légitimer la preuve électronique par le biais d'exceptions au principe de l'écrit signé se sont révélées néfastes. De telles solutions se révélaient limitées lorsque des lois spéciales réclamaient un écrit signé et, plus gravement, militaient pour une acceptation trop large des preuves électroniques sans poser d'exigences de sécurité dans leur confection.

Cela dit, l'équivalence de principe – même conditionnée – des signatures électronique et manuscrite ne clôt point le débat. Bien d'autres questions se trouvent posées au-delà de la réglementation étroite, c'est-à-dire les dispositions du code dans lesquels s'inscrivait jusqu'à présent uniquement la question juridique de la signature. Les points suivants témoignent de cette extension nécessaire du débat.

La normalisation technique : des enjeux de société

La première question renvoie au statut et à l'élaboration des normes. Le contenu des exigences à rencontrer par la signature électronique pour prétendre à la qualité d'une signature manuscrite s'apprécie au regard de l'évolution technologique. Ainsi, la fiabilité d'une signature qui permet l'identification suppose l'utilisation de méthodes cryptographiques toujours plus parfaites et sûres.

« Le contenu de telles exigences s'apprécie à l'égard de l'évolution technologique et des fonctions tirées de chaque concept juridi-

que. Il ne peut être question de fixer, une fois pour toutes, sur la base d'un état donné du développement technologique, les implications précises de chacune de ces fonctions. Ainsi, la fiabilité d'une signature dépendra de l'usage de méthodes de cryptographie toujours plus parfaites et sûres. »¹⁰

La difficulté pour chaque entreprise ou administration qui désire se prévaloir d'une preuve électronique de démontrer le niveau de qualité des mesures de sécurité ainsi exigées se conçoit aisément. En la matière, se développera inévitablement un mouvement en faveur de la normalisation au sein d'institutions *ad hoc* plus souvent privées que publiques. Cette normalisation, sans être obligatoire, représentera cependant un standard acceptable par les tribunaux, sous réserve d'expertise décidée par ces derniers. L'avantage d'une telle normalisation est sa relative souplesse. On sera attentif à la possibilité, y compris pour les représentants des consommateurs, de participer à ces processus de normalisation (voir à cet égard, les statuts de l'Institut européen de normalisation).

Inhérentes à cette normalisation technique, les questions liées au droit de la concurrence et de l'interopérabilité des systèmes s'ajoutent. La normalisation de fait d'un procédé cryptographique peut être l'occasion pour une entreprise de « capturer » un marché. Les exigences d'une normalisation « transparente » et d'une réglementation permettant à chaque opérateur de bénéficier de cette « facilité essentielle » sont à rappeler ici.

Enfin, le développement même des procédés cryptographiques qui fondent les mécanismes de signature justifie d'autres préoccupations : la sécurité publique légitime, dans des conditions procédurales, strictes certes, les écoutes « téléphoniques ». Que devient cet intérêt légitime de l'État si demain des messages indéchiffrables circulent sur nos autoroutes de l'information ? Ce délicat équilibre est à la base des principes directeurs de l'OCDE en matière de cryptographie, principes adoptés le 27 mars 1997.

Où il est question de droits fondamentaux

Le besoin croissant de recourir à la signature électronique pour l'obtention de services de toute sorte, y compris des services administratifs disponibles *on-line* soulèvera d'autres questions : ainsi, celle du droit de chacun à disposer d'une signature électronique,

9. A. Gobert, 1998.

10. Y. Pouillet, 1993, p. 17.

voire de signer anonymement ; celle du droit d'exiger le maintien par les administrations de procédures papier ; celle, enfin du droit, pour chacun de disposer de plusieurs signatures, afin d'éviter que la signature ne devienne un identifiant unique permettant la connexion de nombreux traitements ¹¹. Le groupe d'experts sur le droit du cyberespace réuni sur l'initiative de l'Unesco en septembre 1998 appuie ce droit fondamental des individus au respect de la vie privée, y compris dans la confidentialité des communications par la mise en œuvre de techniques (de cryptographie et d'anonymat) (principe n° 8).

Des nouvelles fonctions de la signature

L'affirmation doit être prise en deux sens : premièrement, la reconnaissance de la signature digitale créera le besoin de nouveaux acteurs dont l'intervention pourra faire l'objet de réglementations ; deuxièmement, la signature digitale opère différemment de la signature manuscrite.

Sur le premier point, on note que la technologie de signature digitale fondée sur un système cryptographique asymétrique suscite l'intervention de nouveaux acteurs, en particulier les autorités de certification qui publient dans des registres ouverts les clés publiques des signataires et attestent de l'authenticité du contenu des informations publiées. Leur intervention fait l'objet de réglementations nouvelles qui décrivent leurs responsabilités et fixent les conditions de la reconnaissance de leurs activités.

Quant au second point, la disparition d'échanges basés sur des relations physiques entre personnes, qui se sont identifiées préalablement, au profit de transactions conclues à travers cet espace virtuel déterritorialisé modifie fondamentalement les caractéristiques de nos relations contractuelles. Cela se répercute notamment sur la fonction de la signature : cette dernière ne peut plus simplement être conçue comme la confirmation *a posteriori* d'une transaction, à des fins de preuve. La signature devient une condition de (re)connaissance d'autrui et, dès lors, une condition d'établissement de la transaction.

Cette reconnaissance d'autrui doit-elle être, encore, nécessairement, celle de personnes physiques ou peut-elle être celle d'une personne morale ? Ce que la signature manuscrite ne permettait pas hier, la signature électronique l'autorise. La personne morale pour-

rait demain disposer au plein sens du terme d'une signature et générer des opérations signées sans devoir s'aider du concours d'une personne physique dans le cadre notamment du fonctionnement d'agents électroniques, c'est-à-dire de systèmes automatisés de prises de commandes ou de facturation.

Premières conclusions : l'éclatement disciplinaire

En conclusion, le droit de la signature électronique invite certes à relire le droit, à approfondir les concepts traditionnels de celui-ci mais aussi, au-delà, à faire éclater les divisions disciplinaires du droit. Le droit de la signature, classiquement question de droit civil des contrats, devient également une question des droits de l'homme (droit à la signature, droit des écoutes téléphoniques, protection de la vie privée), du droit de la concurrence et de la normalisation. Le second exemple démontrera également la nécessité de ce double souci du juriste, confronté aux technologies de l'information et de la communication : relire le droit et être attentif à l'éclatement disciplinaire que la reconnaissance par le droit des technologies de l'information et de la communication y provoque.

1.2. Les ECMS (Electronic Copyright Management Systems) ou la mort du droit d'auteur ?

Présentation des ECMS

Que l'Internet ne soit plus la foire aux idées universitaires, célébrée au temps de sa création, mais devienne chaque jour plus une foire commerciale n'est plus à démontrer. Les systèmes de cryptographie et de signature des œuvres, et, de manière plus générale, les systèmes technologiques (tatouage, etc.) permettront de contrôler l'accès et l'utilisation d'informations enfermées dans des banques de données mieux que dans des coffres-forts ¹².

Ces systèmes, parmi lesquels comptent les systèmes électroniques de gestion des « œuvres », permettent de substituer à la protection assurée classiquement par les droits d'auteur ou, plus récemment, par d'autres droits dits *sui generis*, une protection bien plus efficace à la fois contractuelle et technique, protection qui peut s'appliquer aussi bien à des œuvres effectivement protégées par le

11. Y. Pouillet, 1999, p. 21-28.

12. S. Dusollier, 1999.

droit qu'à toute autre information, pour laquelle le droit ne reconnaît aucune protection ¹³.

Vers la mort du droit d'auteur ?

Sans doute serait-il utile de s'interroger sur les limites de la légitimité de telles protections techniques ¹⁴. Ces protections rendent inutiles les régimes de protection juridique, elles assurent aux détenteurs de simples « biens » informationnels une protection dont l'efficacité et l'ampleur sont sans commune mesure avec celles accordées par le droit de propriété intellectuelle, en exception au principe sacré de libre circulation des idées.

Que deviennent le droit libre de citation, les exceptions au bénéfice de la recherche scientifique, de la copie privée, de l'éducation, etc. si la technologie permet d'interdire toute utilisation non autorisée contractuellement ? N'est-il pas requis, au lieu de saluer la mort des droits de propriété intellectuelle, d'exiger que la technique se conforme à elle ¹⁵ ? En particulier, les droits de citation, les droits des chercheurs scientifiques, voire le droit à la copie privée doivent être reconnus, nonobstant les protections techniques possibles. Plus fondamentalement encore, le groupe d'experts réunis par l'UNESCO au mois de septembre 1998 recommandait aux États de maintenir, voire de développer un « domaine public » en ce qui concerne l'information essentielle aux citoyens : « Il incombe aux organismes publics d'intervenir pour faire en sorte que l'information publique soit largement disponible sur l'Internet et veiller à son exactitude et à sa diffusion en temps utile. Cette information pourrait comprendre les informations officielles, les informations concernant le patrimoine culturel et les informations archivistiques et historiques. » ¹⁶ (principe n° 9).

13. Le Parlement européen et la Directive du Conseil 96/9/EC du 11 mars 1996 sur la protection juridique des bases de données, *Journal officiel de la Communauté européenne*, juin 1993, L. 77 considèrent que l'investissement du marché (en termes de ressources financières, de temps et d'énergie) à obtenir, vérifier et présenter les contenus d'une base de donnée doit être protégé par un nouveau droit économique.

14. P. Samuelson, 1996.

15. S. Dusollier, 1999.

16. Voir Annexe, p. 5-6, § II. A. 9 et *Rapport de la réunion d'experts sur le droit du cyberspace*, 1998.

Le développement de vastes systèmes d'ECMS invite à d'autres considérations : qui gèrera ces systèmes ? Quel rôle faut-il reconnaître aux sociétés de droit d'auteur ? À nouveau, les questions de concurrence et de normalisation, en particulier à propos de la codification des œuvres, se trouvent soulevées.

Enfin, l'utilisation de tels systèmes sera génératrice de données nominatives et il importera de déterminer quel droit d'utilisation de ces données sera reconnu aux divers acteurs intervenants, depuis les gestionnaires du système jusqu'aux auteurs eux-mêmes.

Du service au produit informationnel

On achèvera les considérations relatives à ce second exemple par quelques remarques à propos de la responsabilité du fait des banques de données accessibles *on-line*.

Traditionnellement, l'activité de renseignements a été analysée comme un service, le fournisseur de ce service devant mettre à la disposition de son client la diligence requise. L'interposition entre le producteur d'informations et l'internaute d'un outil technique capable de répondre de manière standard à des demandes variées d'information contribue à analyser différemment l'opération et, comme le montre la jurisprudence récente, à s'interroger en cas d'informations incomplètes ou, inexactes sur la qualité du « produit informationnel ». Par « produit informationnel », on entend cet ensemble intégrant à la fois, d'une part, les dispositifs techniques (logiciel, programmation, etc.) et organisationnels (mode et qualité de la collecte) et, d'autre part, le contenu (caractère complet, mise à jour, etc.). Il s'agira en effet de s'interroger sur la conformité de ce produit à l'attente légitime de l'internaute ¹⁷.

En un mot, c'est clairement en termes de qualité du produit et non plus de diligence de services que s'examinera la responsabilité des producteurs voire des distributeurs d'informations.

Labélisation des sites, techniques de filtrage : la technique au secours du droit

Dans ce contexte, s'explique la tendance à développer comme pour d'autres produits de consommation des techniques de labélisation (voir notamment les labels nord-américains : Webtrust, Truste) et, à partir de là, de filtrage, tels les PICS (Platform for Internet Con-

17. E. Montero, 1998.

tent Selection), voire en outre de négociation tel le P.3.P (Platform for Privacy Preferences). L'idée est simple. Chaque « produit informationnel » peut être examiné du point de vue de sa conformité à des standards de décence, de violence, de respect de la vie privée (voir, à ce propos, Truste), de protection des consommateurs. Cette labélisation opérée *a priori*, couplée ensuite à des techniques de filtrage, permet à l'internaute de sélectionner les sites suivant ses préférences, voire de négocier avec eux une protection particulière ou, à l'inverse, renoncer à celle-ci ¹⁸.

Sans doute, le droit de la labélisation est-il encore à écrire : quels seront les critères pour apprécier si tel ou tel site a droit au label ? Peut-on imaginer une certaine concurrence des critères ? Quelle transparence des critères exiger ? Quelle est la responsabilité des organismes qui délivrent de tels labels ? Quel rôle l'État doit-il jouer dans la reconnaissance des organismes habilités à délivrer les labels et dans la fixation des critères d'octroi du label. À quelle reconnaissance légale des labels faut-il procéder ? Et, finalement, quelle sanction proposer en cas de non-respect des conditions de celui-ci ? ¹⁹.

Secondes conclusions : de l'interaction entre droit et technologie

Sans doute faut-il constater que la technologie permet de renforcer l'effectivité du droit qui, sans elle, resterait lettre morte ou trouverait difficilement à se satisfaire des procédures judiciaires classiques du droit peu rapides et peu efficaces. Ainsi l'existence d'un site révisionniste sera-t-elle plus facilement contrée par les mécanismes de filtrage ou de blocage d'accès comme prévu par les « Chartes de l'Internet » que par la condamnation d'un tribunal à propos d'un site insaisissable voyageant sur la toile mondiale du Web. Dans un autre ordre d'idées, les ECMS, avons-nous dit, protègent plus efficacement les droits d'auteur que nos législations. Ces constatations amènent certains auteurs à préférer aux lois étatiques classiques le procédé de ce qu'ils appellent la *lex informatica* ²⁰.

Élargissons le propos pour souligner les diverses facettes de l'interaction entre le droit et la technologie. En effet, c'est tantôt les acteurs eux-mêmes qui réclameront l'intervention du droit pour con-

sacrer la valeur de solutions techniques, tantôt c'est le droit lui-même qui réclamera des acteurs la prise de mesures techniques, notamment afin de rendre effectif le respect de la loi ²¹.

Le premier rôle, c'est-à-dire la consécration de solutions techniques, est sans conteste celui qui est réclamé par les promoteurs des services susceptibles d'être offerts grâce à l'Internet. Ainsi, en matière de signature électronique, premier exemple analysé, la nécessité de sécuriser le commerce dans des réseaux ouverts comme Internet justifie la requête des fournisseurs de services de voir reconnus des services de certification électronique, les « Certification Authorities », ou bien les fameux notaires électroniques ou « Trusted Third Parties ». La fonction des premiers s'est trouvée légalisée dans quelques États (Utah et Floride aux États-Unis d'Amérique, Allemagne, Italie) ou s'apprête à l'être ainsi au niveau européen par la proposition de directive sur un cadre commun en matière de signatures électroniques. À propos des services électroniques de gestion des droits d'auteur (les « Electronic Copyright Management Systems – ECMS »), la récente réforme de la Convention de Berne sur le droit d'auteur criminalise toute manœuvre visant à déjouer les protections techniques offertes par ces services de gestion.

À l'inverse, le droit peut réclamer la prise de solutions techniques soit de manière vague et indirecte, soit de manière directe et précise. Ainsi, l'application du principe de responsabilité conduira le juge à sanctionner sur le plan civil voire pénal les fournisseurs d'accès et les serveurs qui n'auraient pas pris les mesures de sécurité qui, selon les règles de l'art, s'imposent pour prévenir les dommages susceptibles d'être encourus par les utilisateurs de leurs services. Rappelons à ce propos que c'est en réponse à la crainte d'une intervention législative, le fameux « Decency Act », que les industriels américains ont, notamment, développé le standard de filtrage, la « Platform for Internet Content Selection » (PICS) dont nous parlions plus haut.

Sans doute, est-il important que devant les normes techniques développées qu'elles soient « privacy », « copyright », « consumer protection », « enhancing protection », le juriste analyse avec soin la manière dont ces mesures techniques respectent les standards légaux à la fois dans la lettre et dans l'esprit, ce qui n'est pas toujours le cas. Ainsi en est-il des ECMS dont la protection ne respecte pas nécessairement l'équilibre qui gouverne la reconnaissance des pré-

18. J.-M. Dinant, 1997 et 1999 ; J. Reidenberg, 1998.

19. Voir sur toutes ces questions S. Louveaux, Y. Pouillet et A. Salaun, 1999.

20. J. Reidenberg, 1996.

21. Y. Pouillet et R. Queck, 1997.

rogatives des auteurs, et en matière de *privacy*, à propos du P.3.P. qui permet, dans tous les cas de négocier, y compris les droits inaliénables liés à la protection de ses libertés²². Il s'agit donc bien que la technique respecte le droit.

2. LES DIVERSES TECHNIQUES DE RÉGLEMENTATION DE L'INTERNET ET LE RÔLE DU DROIT ÉTATIQUE

Position du problème

La technique peut être, nous l'avons vu (p. 13), un mode de réglementation des comportements sur les autoroutes de l'information. Il en est d'autres avec lesquels le Droit entretient également un dialogue.

Un premier temps vise à identifier les diverses techniques de réglementation applicables à l'Internet ou plus largement aux autoroutes de l'information ; le second temps analyse les modes de réception par le droit étatique ou supra-étatique de ces diverses techniques de réglementation et envisage quelques critères qui permettraient de légitimer les modes de réglementation non étatiques.

2.1. De la diversité des modes de réglementation

Considérations préliminaires

Une réglementation a pour but de prescrire des normes de comportement. Cela dit, on reconnaît la diversité des modes de production et d'application des normes selon quatre critères : l'objet, l'auteur, le sujet et la sanction de la norme.

On notera, en outre, que la dimension internationale de l'Internet conduit à une certaine concurrence entre les divers ordres réglementaires nationaux. Lorsqu'un État veut réglementer tel comportement, il est loisible et facile pour les acteurs de déplacer leurs activités vers un autre État et de préférer y retrouver un cadre plus souple et moins contraignant. Ce phénomène de « *dumping réglementaire* » est réel²³. À l'inverse, on notera l'avantage que peut avoir pour le consommateur de préférer la sécurité que lui confère un environnement réglementaire plus soucieux de ses intérêts. Ce second aspect ne doit pas être négligé.

22. J.-M. Dinant, 1999.

23. Y. Pouillet et R. Queck, 1997.

Une énumération

Il est impensable d'énumérer les multiples sources normatives du droit de l'Internet. Aux sources publiques du droit, c'est-à-dire les normes étatiques nationales et internationales, on oppose souvent celles privées, fondées tantôt sur la liberté contractuelle, tantôt sur ce qu'il est convenu d'appeler l'autoréglementation qui s'exprime par des « codes de conduite » ou « chartes ». On ajoutera à ces sources la certification et les usages dans lesquels certains voient une « *lex electronica* », parallèle à la « *lex mercatoria* » mais développée dans un contexte électronique. On ajoutera que la technologie elle-même (voir *supra*, « Secondes conclusions » § 1.2.) peut également être une source de normalisation des comportements.

À propos de ces sources privées, on note que les acteurs ne se contentent pas de définir un contenu aux normes qu'ils entendent suivre mais surtout qu'ils mettent sur pied des moyens pour assurer la mise en œuvre du contenu de cette autorégulation (problème de l'effectivité des normes). Ainsi, les modérateurs nommés au sein des groupes de discussion sont chargés de veiller à une certaine police des messages en conformité avec la réglementation de la *news group* à laquelle les participants ont adhéré. Des sanctions propres aux réseaux comme la déconnexion et le « *flaming* » ressemblent étrangement à des pratiques de justice privée. Les « *hot lines* » créées dans le cadre de certains codes de conduite pour permettre de dénoncer des agissements contraires aux codes de conduite constituent d'autres exemples de procédures mises en œuvre pour assurer une discipline du réseau. Plus intéressants encore, les mécanismes de « *labels* » ou de « *ratings* » mis au point sur certains serveurs (voir *supra*, « Labellisation des sites » § 1.2) garantissent et informent les utilisateurs de la qualité des services proposés (ainsi, le label « *privacy friendly* » ou celui apposé sur certains sites d'informations journalistiques garantissant le respect de la déontologie de la presse). La valeur de tels classements ou labels dépendra évidemment de l'instance qui y procède. À propos de l'autorité chargée de la mise en œuvre du respect de la norme, il convient de mentionner également les initiatives nord-américaines de créer des mécanismes non judiciaires de résolution des conflits (les « *Alternative Dispute Resolution* »), en particulier représentés par les « *virtual magistrates* ». Ces derniers désignent des personnes physiques, arbitres ou simples médiateurs, accessibles via le réseau et habilités à régler les conflits nés au sein des réseaux, qu'il s'agisse de problèmes de diffamation, d'ingérence dans la vie privée ou de non-respect des règles propres à un « *news group* ».

En un mot, les sources privées de réglementation mettent en place des mécanismes d'expression des règles, de contrôle de leur application et finalement de sanction de leur non-respect, sanctions prononcées par leurs propres « magistrats ». Les divers moyens décrits ci-dessus peuvent exister séparément ou, au contraire, se cumuler : un code de conduite fera référence au fait que seuls des sites labellisés peuvent souscrire au code de conduite dont le respect sera assuré par la possibilité de recourir à des cybermagistrats. Les réflexions qui suivent développent quelques remarques sommaires à propos de ces diverses sources privées ou publiques.

2.1.1 Les normes étatiques

À propos des normes étatiques

Que l'État nation constitue une instance légitime d'expression de la régulation de l'Internet est évident. Les modes d'élaboration de la norme sont soigneusement décrits dans des textes et les procédures qui entourent cette élaboration ; ils garantissent donc une discussion démocratique. L'application de la norme est confiée à des juridictions « professionnelles », entourées de garantie d'indépendance et de fonctionnement contradictoire.

À propos des « environnements électroniques », selon l'expression de Pierre Trudel²⁴, on notera deux tendances particulières du droit étatique : d'une part, celle de préférer le recours à des notions à contenu vague, évolutif et susceptible de multiples interprétations, des « standards » et, d'autre part, celle de confier l'interprétation de ces standards à des organes-relais, parfois qualifiés d'autorités administratives indépendantes. Ainsi, pour reprendre l'exemple de la Belgique – mais cet exemple peut-être étendu à l'ensemble des pays de l'Union Européenne –, la loi reconnaît, en matière de *privacy*, l'existence d'une autorité de contrôle : La Commission de protection de la vie privée ; en matière de réglementation de l'audiovisuel, un organe de réflexion et de fixation de certaines règles relatives au contenu des émissions et chargé de veiller au pluralisme culturel et d'opinions : le Conseil supérieur de l'audiovisuel ou le mediaraad ; enfin, à propos des services de télécommunications existera une autorité de contrôle du secteur : L'Institut belge des postes et télécommunications²⁵.

La dimension internationale des autoroutes de l'information conduit les États à rechercher, au sein d'instances internationales, des

modes d'élaboration du droit ou de coopération des autorités chargées de l'application de droits restés nationaux²⁶. Qu'il s'agisse de conventions internationales comme celles de l'ONU, de l'UIT, de l'OMC, de l'OMPI, de l'OCDE, d'organes comme ceux du G7, qu'il s'agisse de conventions d'entraide policière, chargés de lutter contre la délinquance informatique (voir à ce propos, la proposition de Charte internationale sur l'Internet présentée par la France à l'OCDE), nombre d'initiatives publiques sont prises pour maintenir le rôle de l'État dans la protection et la sauvegarde des droits des individus et des intérêts supérieurs de la société. Certains²⁷ proposent même la création d'une « Autorité internationale du cyberspace », en réaction aux mouvements d'émancipation du droit de l'Internet et face à la puissance croissante des normes privées dont nous allons parler maintenant. C'est à cette autorité et à la nécessité de fixer des règles globales pour le commerce électronique mondial que fait référence le « Global Business Dialog » prôné par M. Bangemann, Commissaire à l'Union Européenne.

2.1.2. Les normes privées

À propos du contrat

L'interactivité des réseaux donne au consentement de l'internaute des potentialités d'application sans précédent. Qu'il s'agisse d'accepter ou non des cookies, de consentir à tel ou tel traitement, de révéler ou non son identité, de s'opposer à l'envoi de courrier non sollicité, la technique offre à l'internaute la possibilité de prendre ses propres responsabilités²⁸. Tentés par ce paradigme contractuel propre à l'environnement de l'Internet, certains auteurs estiment qu'à la responsabilité de l'État de réglementer les comportements, il est possible désormais de substituer celle du citoyen, qui, par son consentement ou ses consentements successifs, autorisera ou non telle ou telle opération.

Les principes d'autonomie de la volonté et de la convention-loi, unanimement reconnus par tous les ordres juridiques, donne à cette approche fondée sur la responsabilité individuelle des internautes, un poids considérable. L'approche contractuelle exige bien évidemment que la technologie permette de tels choix. Ainsi les questions : l'internaute souhaite-t-il être identifié ? Pour quels types de finalités ?

24. P. Trudel, 1997.

25. Y. Pouillet, 1993.

26. B. Frydman, 1997.

27. J.-J. Lavenue, 1996.

28. R. Dunne, 1994 ; P. Trudel, 1996.

Pour quelle durée ? Devraient-elles faire l'objet de pages écran et la configuration du système devraient garantir le respect de tels choix.

À propos de l'autoréglementation

Pierre Trudel²⁹ définit l'autoréglementation comme « les normes volontairement développées et acceptées par ceux qui prennent part à une activité ». On connaît la multiplication de ces codes, parfois conclus localement dans une université, dans un *news group*,..., parfois plus largement pour un secteur d'activités (le marketing direct), voire pour l'ensemble des activités opérées sur le Net (les Chartes nationales comme la charte française de l'Internet ou le Code of Conduct néerlandais sur le commerce électronique en voie d'adoption). L'Internet Society, organisme purement privé chargé d'assurer la coopération et la coordination internationale entourant la technologie et les programmes du réseau Internet, publie des lignes directrices relatives à l'utilisation de l'Internet et à l'utilisation du réseau. Son Président, V. Cerf, affirme à cet égard : « Il n'est plus justifié de fonder les codes de conduite sur la seule base des intérêts de ceux qui paient pour l'infrastructure ou les systèmes d'information. Même si cette question est sensible, la diversité des éléments constitutifs de l'Internet fait de ces seuls intérêts une base faible pour formuler des manières d'agir. Ainsi les codes de conduite ne doivent être élaborés et motivés que partiellement en prenant en compte les intérêts propres des différents acteurs. Nombre de suggestions reprises ci-dessus sont fondées sur la théorie suivant laquelle la mise en lumière des intérêts propres de chaque acteur peut informer et influencer les choix de comportement. »³⁰

La justification de cette autoréglementation galopante est triple. À l'argument du caractère technique et évolutif de l'objet – que ce mode de régulation doit prendre en compte –, s'ajoute celui de la qualité des auteurs, seuls capables de percevoir les enjeux des solutions et d'autant plus enclins à respecter la règle qu'ils l'auront eux-mêmes formulée. Autre argument plus important encore, celui de l'adéquation et de l'effectivité des sanctions proposées par l'autoréglementation : le blocage immédiat par l'ensemble des fournisseurs d'accès d'un site dénoncé par le mécanisme d'une *hot line* constitue la réponse appropriée et efficace à l'existence d'un site pornographique, bien plus qu'une condamnation juridictionnelle³¹. La possibilité de leur élaboration

à un niveau mondial apparaît comme un argument supplémentaire au moment où la dimension globale des problèmes posés par les autoroutes de l'information est incontestée.

Au-delà de l'élaboration des normes, l'autoréglementation prétend aujourd'hui offrir des modes d'application de la norme dans les communautés virtuelles distinctes des communautés spatiales localisées dans des territoires donnés et soumis aux juridictions étatiques. On connaît depuis longtemps le rôle que peuvent ainsi jouer les modérateurs de réseaux, les premières expériences de « *cybermagistrates* », tribunaux virtuels, chargés de régler les litiges apparus dans le monde virtuel et la création de conseils chargés d'appliquer les chartes de l'Internet constituent des démonstrations supplémentaires de l'aptitude de l'autoréglementation non seulement à élaborer avec souplesse le droit de l'espace virtuel mais en outre à le sanctionner³². La tentation est forte d'y voir une source non plus complémentaire du droit étatique mais remplaçant ce dernier³³ ou en tout cas dispensant l'État d'une intervention réglementaire tatillonne. Tantôt, la norme privée dispense de la norme étatique : ainsi, la manière dont est réglée actuellement la délicate question de l'attribution des noms de domaine sur l'Internet témoigne tout au moins de l'autosuffisance des solutions autoréglementaires³⁴. Tantôt, et c'est le cas dans le débat qui oppose l'administration américaine à l'administration européenne en matière de protection des données, le code de conduite, la norme privée même fortement appuyée voire initiée par les pouvoirs publics américains permettent à ces derniers de ne pas mettre en place un appareil réglementaire et administratif lourd et qualifié d'inutile au-delà de l'affirmation de principes légaux par ailleurs reconnus depuis toujours par les tribunaux³⁵.

32. H.H. Perritt, 1993 ; R. Dunne, 1994.

33. D. Johnson et D. Post, 1996.

34. A. Wilkinson, 1998.

35. Après la mise en application (25.10.98) de la Directive européenne sur la protection des données à caractère personnel (95/46/EC), la Commission européenne et le Department du commerce des États-Unis d'Amérique sont entrés en contact en vue d'élaborer un cadre juridique pour le transfert de ces données aux États-Unis. À cet effet, le Department of commerce a publié les « Safe Harbor' privacy principles » les 15 et 16 novembre 1999. Si la Commission européenne estime que lesdits principes sont acceptables, alors une décision pourrait être prise (dans le cadre de l'article 25.6 de la Directive sur la protection des données) reconnaissant ceux-ci comme offrant une protection adéquate pour le transfert des données à caractère personnel de l'Europe aux États-Unis ; voir B. Gellman, 1998.

29. P. Trudel, 1989.

30. P. Trudel, *op. cit.* Cité par V. Cerf, 1994.

31. T.I. Hardy, 1994.

À propos de la certification

Dans un monde global où le réseau constitue la seule manière d'entrer en communication, la certification qui se définit comme une procédure par laquelle un tiers garantit la qualité spécifique d'une personne ou d'un produit, apparaît comme une solution heureuse.

La certification a pour ambition de rassurer l'internaute non seulement sur l'existence, l'identité et l'adresse de l'interlocuteur, voire sur sa qualité professionnelle (voir à cet égard, *supra*, la signature électronique), mais, au-delà, garantit la conformité de ses produits ou services à telle norme de qualité, de ses traitements à telle législation protectrice de la vie privée, de ses pratiques à celle exigée en matière de protection des consommateurs ; enfin, la certification peut attester de la sécurité générale du site. Autant de questions qui pourront faire l'objet de certificats spécifiques (par ex. le label délivré par l'ICPA (Internet Consumer Protection Agency) traite les questions de conformité aux seuls standards de vie privée) ou plus globaux (ainsi, l'initiative « Webtrust » développé par l'Accountants'Association américaine qui vise les diverses questions évoquées ci-dessus).

La certification présente une solution qui peut être complémentaire soit à une source normative étatique, soit à l'autorégulation, dans la mesure où elle se réfère soit à une loi, soit à un code de bonne conduite. Elle repose essentiellement à la fois, d'une part, sur la qualité (indépendance, expertise) des autorités de certification et des procédures de vérification et, d'autre part, sur la responsabilité effective de ces autorités en cas de délivrance induite d'un certificat. Enfin, la certification permet des sanctions faciles et efficaces, dans la mesure où l'entreprise et l'individu craignent le retrait du certificat et la publicité qui s'attache à un tel retrait ³⁶.

À propos des « usages » ou de la « lex electronica »

Au-delà des sources codifiées et bien identifiées dont nous venons de parler, il faut évoquer les principes plus diffus parfois présents dans les « Acceptable Use Policies » proposées par les fournisseurs d'accès ou les serveurs, et les « Netiquette », sorte de « 10 commandements » ou de règles fondamentales du permis de conduire sur Internet ³⁷.

Ces règles s'énoncent comme suit :

1. Tu n'utiliseras pas un ordinateur pour nuire à autrui.

36. Y. Pouillet et J. Royen, 1998.

37. A. Rinaldi, 1995.

2. Tu n'interféreras pas avec le travail d'autrui.
3. Tu ne fureras pas dans les fichiers d'autrui.
4. Tu n'utiliseras pas un ordinateur pour voler.
5. Tu n'utiliseras pas un ordinateur pour porter un faux témoignage.
6. Tu n'utiliseras pas et ne copieras pas de logiciel pour lequel tu n'as pas payé.
7. Tu n'utiliseras pas les ressources de l'ordinateur d'autrui sans autorisation.
8. Tu ne t'approprieras pas les créations intellectuelles d'autrui.
9. Tu envisageras les conséquences sociales du programme que tu écris.
10. Tu utiliseras un ordinateur d'une manière qui montre considération et respect.

À propos de la contravention à ces règles, on notera que les sanctions peuvent être des réactions organisées ou non : le « flaming », la déconnexion de l'utilisateur indélicat, la menace de contacter les autorités policières,...

La comparaison entre ces « usages » spontanément élaborés par les communautés virtuelles et les règles de conduite habituellement pratiquées par les communautés de marchands conduisent à rapprocher cette « *lex electronica* » de la « *lex mercatoria* » ³⁸. Le rapprochement est d'autant plus séduisant que certains dénoncent le discours économiste dominant qui « conduit à soumettre la société de l'information en général et les activités sur l'Internet en particulier à la seule loi du marché mondial » ³⁹.

Ce parallèle tentant autorise les réflexions qui vont suivre sur le rôle du droit étatique face aux diverses techniques de réglementation.

2.2. Du rôle du droit étatique dans la réception et la promotion des sources « privées » du droit du cyberspace.

Réflexions préliminaires : la nécessité d'un dialogue

Pierre Trudel, paraphrasant un propos de H.H. Perritt, écrivait : « Les acteurs engagés dans les transactions internationales, par

38. B. Wittes, 1995.

39. B. Frydman, 1997 ; voir aussi J.N. Brouir *et al.*, 1996.

exemple, ont développé des pratiques qui sont créatrices de droit. Il y aurait là des analogies intéressantes à faire sur le plan de la réglementation des environnements de commerce électronique quoi qu'on ne peut, à l'heure actuelle, parler de l'émergence d'un véritable corpus de règles d'application générale. L'avènement de cette normativité serait favorisé par le développement de pratiques plus généralisées d'arbitrage international effectué sans égard aux différents droits nationaux. Or, même si les usages et pratiques dans un champ d'activité donné, sont souvent pris en compte et, ainsi, intégrés, en quelque sorte, au droit étatique, l'intérêt de ce type de norme réside dans sa capacité à organiser de façon autonome les comportements et les transactions des membres d'une communauté. Le respect des usages et pratiques est, dans de telles circonstances, la condition essentielle de l'adhésion d'un participant à une communauté donnée. Toutefois, si l'importance de la communauté le justifie, les usages et pratiques pourraient constituer une technique de réglementation complète, parallèle au droit étatique, qui réglerait les rapports des participants d'une communauté et qui serait administrée par ses propres instances. Le modèle de la *lex mercatoria* du Moyen âge est souvent cité en exemple. On observe plusieurs débats sur l'opportunité de développer un cadre juridique analogue pour le cyberespace. »⁴⁰

La réflexion doctrinale sur la *lex mercatoria* a permis à nombre d'auteurs d'y voir l'occasion d'une reconnaissance claire et indiscutable du pluralisme juridique. Élargissant le propos, F. Rigaux (1977) écrit : « Le citoyen d'un État possède des biens ou réside sur le territoire d'un autre État, il est membre d'une confession religieuse organisée, appartient à des groupements professionnels transnationaux. La loi de chacun des États auxquels il est soumis, le droit de l'Église à laquelle il est affilié, les engagements souscrits dans l'exercice des pouvoirs économiques privés qui lui appartiennent, forment autant d'ordres juridiques distincts, imparfaitement ordonnés l'un à l'autre. »⁴¹

Dans cette perspective, l'acte d'autorégulation et, plus généralement, les sources privées du droit que d'aucuns qualifient de droit « mou » (*soft law*) apparaissent au plein sens du terme comme des ordres juridiques même si leur production peut paraître moins légitime qu'une élaboration publique plus traditionnelle.

40. P. Trudel, 1997.

41. Rigaux, 1977, p. 439.

Par ailleurs, sans naïveté, il faut bien reconnaître qu'une telle autoréglementation par les acteurs eux-mêmes de leur propre activité est loin d'être gratuite. Il s'agit pour ces opérateurs d'éviter les réglementations étatiques ou de leur donner une interprétation « molle », notamment pour éviter de graves accusations. Le débat relatif à la pornographie sur l'Internet suscité par quelques drames récents et la multiplication d'autoréglementations en la matière qui s'en est suivie, illustre bien le propos.

2.2.1. La « réception » par le droit étatique des sources privées

Le rappel des trois lois : contrat, concurrence et responsabilité

Le rappel des principes généraux et universels du droit étatique, en particulier l'autonomie contractuelle, la concurrence et la responsabilité peuvent constituer un premier mode de contrôle des sources privées du « Cyberdroit ».

À cet égard, on s'interrogera sur la portée que les auteurs de ce cyberdroit privé assignent à leur autoréglementation. Traditionnellement, un code de conduite avait pour objet de régler le comportement entre les acteurs qui coopéreraient à cette œuvre normative. Il s'agissait de fixer les règles du jeu entre acteurs et d'éviter à chacun les effets d'une concurrence sauvage. Incidemment, le code de conduite pouvait avoir une portée externe, en bref prétendre à des effets en dehors du cercle de ses destinataires naturels, c'est-à-dire les auteurs même de l'autoréglementation ou les personnes représentées lors de son élaboration. Ainsi, en définissant les comportements admis par la profession ou certains acteurs de celle-ci, l'autoréglementation entendait fixer des règles de conduite vis-à-vis des tiers concernés par leurs opérations, en particulier, mais non nécessairement les personnes amenées à contracter avec eux. Ainsi, si une association de marketing direct s'interdit ou au contraire s'autorise certains comportements publicitaires, cette attitude peut affecter les tiers indépendamment du fait que certains de ces tiers peuvent devenir des contractants. L'opposabilité d'un code de conduite par rapport à de tels destinataires externes est plus discutable.

À propos de cette dernière hypothèse où le tiers n'est pas simple tiers mais contractant et se voit opposer le contenu du code de conduite comme norme contractuelle, sans doute suffira-t-il pour le juge d'aller « jusqu'au bout de la logique contractuelle », comme l'affir-

maît M. Vivant⁴², pour noter l'absence d'un consentement total et éclairé de la part de l'internaute dans l'acceptation d'une « *policy* » ou d'un Code of conduct peu respectueux de ses intérêts. Se retrouve ici la double question du contenu de la norme privée, de sa clarté, de son caractère ou non abusif et de l'intégration de celle-ci à l'accord de volonté lorsque la référence au code de conduite fait l'objet d'un hyperlien peu facile à apercevoir.

À propos des autres tiers qui pourraient se prétendre lésés par un comportement pourtant conforme à un code de conduite, le recours à des standards comme celui de la « bonne foi », du « bon père de famille », des « règles de l'art » permettront de saluer l'adoption d'un code de déontologie respectueux de ces normes de prudence et de diligence, et de sanctionner la violation de la norme élaborée par l'ordre juridique privé dans la mesure où cette norme constitue un standard professionnel et sa violation automatiquement une faute⁴³. Au contraire, le recours aux standards autorisera la dénonciation d'autoréglementation ou de systèmes de certification dont le contenu ou les procédures apparaîtront ne pas respecter de tels standards.

Au sein d'un secteur, l'adoption par un groupement de « codes de conduite » ou de « normes techniques » peut avoir pour objectif de « préjudicier » un concurrent ou des membres du groupement particulièrement désarmés. Il suffira alors de rappeler les principes de la concurrence pour ôter au code de conduite toute valeur ou, à l'inverse, de saluer dans le contenu du code l'expression d'une saine concurrence et du respect d'usages loyaux et honnêtes de la profession.

Le rejet de l'ordre juridique privé pour violation de l'ordre public

La nombreuse jurisprudence relative aux activités des ordres associatifs à la fois lors de la fixation des règles disciplinaires et lors de leur application permet de dégager quelques règles applicables également en matière d'autoréglementation du cyberespace. Il s'agit là également d'ordres juridiques privés dont le pouvoir créatif de normes n'est pas contesté. Or, sans contester l'autonomie des normes édictées par la profession, la jurisprudence les a parfois remis en cause, en particulier pour les deux motifs suivants la jurisprudence :

– tout d'abord, quand la norme professionnelle est en conflit avec une norme étatique jugée d'ordre public. Ainsi, un code de

conduite autorisant un serveur à traiter les données obtenues par *cookies*⁴⁴ sans information préalable de l'internaute serait contraire au principe de transparence, affirmé par la directive de protection des données. Aussi, le champ laissé à l'autorégulation se réduira chaque fois qu'au nom de motifs supérieurs ou de valeurs fondamentales, le droit étatique édictera ou reconnaîtra des normes comme étant d'ordre public. Cette assertion doit cependant être nuancée par la considération suivante : l'effectivité de la norme étatique peut être réduite de par le fait que l'ordre étatique ne disposera pas des moyens de la faire respecter. Dans une telle hypothèse, la norme étatique aura un caractère plus symbolique qu'une portée réelle et l'autorégulation peut constituer un moindre mal ;

– deuxièmement, soit parce que l'application de la norme représente un abus de droit dans la mesure où la sanction est démesurée par rapport à la violation ou que le prononcé et la procédure qui y mènent ne respectent pas les droits de la défense selon les principes généraux de l'article 6 de la Convention européenne des droits de l'homme. Cette question est particulièrement sensible lorsque l'autoréglementation prétend à des effets externes, par exemple lorsqu'elle traite des questions de protection des données ou de consommateurs. À cet égard, on relèvera la disposition particulièrement heureuse de l'article 17 de la proposition de directive en matière de commerce électronique : « Les États membres veillent à ce que les organes de résolution extrajudiciaire des conflits de consommation, appliquent dans le respect du droit communautaire, les principes d'indépendance, de transparence, du contradictoire, de l'efficacité de la procédure, de la légalité de la décision, de la liberté des parties et de représentation. »⁴⁵

En ce sens, dans le contexte de l'Internet, bien des sanctions appliquées unilatéralement des organes peu transparents et sans contrôle externe pourraient apparaître comme des abus de droit : ainsi, le retrait immédiat d'une certification pour une soi-disante non-conformité de comportement d'un serveur avec les règles d'un code de conduite peut apparaître comme une forme de censure inacceptable par un ordre étatique, soucieux du respect de la liberté d'expression ou du principe du contradictoire.

44. Les « *cookies* » sont des agents permettant de retracer, à l'aide de l'information collectée sur un site web, les usagers et de localiser les ordinateurs.

45. N. Decoopman, 1989.

42. M. Vivant, 1997.

43. F. Osman, 1995.

2.2.2. *La promotion de l'ordre juridique privé : réflexions autour de la directive 95/46 sur la protection des données*⁴⁶

Deux modes de promotion

À partir de deux dispositions de cette directive, nous souhaiterions montrer, à la suite de l'article 27, comment le droit étatique peut articuler normes publiques et normes privées et promouvoir ainsi l'adoption de ces dernières ; et, comment, à la suite de l'article 25, un ordre juridique national, tout en assurant le respect de la culture et des systèmes d'autres ordres juridiques, peut fixer certains critères pour la reconnaissance de normes privées produites dans ces autres ordres juridiques.

« Des codes de conduite sous contrôle »

L'article 27, § 1, de la directive affirme que les États membres et la Commission « encouragent » l'élaboration de codes de conduite destinés à contribuer en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales. Les rédacteurs de tels codes pourront les soumettre aux autorités de contrôle qui en vérifieront la conformité au regard de la réglementation.

Le texte envisage également l'élaboration de codes communautaires qui peuvent, quant à eux, être soumis au groupe européen de protection des données qui examinera notamment s'ils respectent les dispositions nationales.

Lorsque des codes seront soumis à leur approbation, tant l'autorité nationale de contrôle que le groupe européen pourront recueillir, « s'ils l'estiment opportun », les observations des personnes concernées ou de leurs représentants. En outre, selon qu'il s'agira d'un code national ou communautaire, chacune de ces instances pourra respectivement en assurer la publicité⁴⁷.

Le principe de la directive est simple : l'autorégulation comme la certification constituent en aval des principes de la directive des outils efficaces de la mise en œuvre de tels principes. Ils contribuent

46. Directive 95/46/CE du Parlement européen et du Conseil du 24.10.95 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Journal officiel de la Communauté européenne* du 23.11.95 n° L281, p. 31.

47. M.-H. Boulanger *et al.*, 1997.

à améliorer l'image de marque de celui qui s'y soumet et accroissent la confiance de l'internaute. Leur souplesse et leur spécificité les rendent aptes à offrir des solutions évolutives adaptées aux particularités de chaque secteur. Enfin, leur caractère européen permet de garantir une équivalence de protection à propos des traitements opérés en quelque coin de l'Europe.

La reconnaissance par l'ordre étatique de ces codes de conduite s'opère de deux manières :

- premièrement, la procédure formelle d'« homologation » s'opère non seulement au regard des critères de fond que constitue le respect des dispositions de la directive mais également de critères plus procéduraux : publicité du contenu de l'autoréglementation ou des critères de certification, transparence et ouverture des débats en prenant en compte la variété des acteurs intéressés par les traitements, y compris, en particulier, les personnes concernées ;
- deuxièmement, les codes de bonne conduite n'exemptent pas les secteurs de l'application des législations nationales issues de la directive qui garantiront, en termes généraux certes, le respect des droits subjectifs et les possibilités de recours des personnes concernées. Cette soumission à la loi, en définitive, apporte aux codes sectoriels, ne fût-ce qu'indirectement, une effectivité certaine, étant donné que la loi s'accompagne de force juridique contraignante qui reste l'ultime garantie de l'efficacité des principes énoncés.

La recommandation du Conseil de l'Europe du 24 septembre 1998 (Doc. 98/560/CE) relative au développement de la concurrence en matière d'audiovisuel et de l'industrie des services d'information par la promotion de cadres nationaux aptes à assurer un niveau comparable et effectif de protection des mineurs et de la dignité humaine va plus loin encore, dans la mesure où son annexe fixe des lignes directrices « indicatives » destinées à promouvoir l'autoréglementation. Ces lignes réclament que l'autoréglementation s'appuie sur une participation complète et transparente de toutes les parties intéressées (autorités publiques, consommateurs, utilisateurs et industries) à la rédaction, à la mise en œuvre et à l'évaluation des codes de conduite. Seule cette participation peut légitimer le caractère volontaire et privé des codes de conduite.

La proposition amendée en vue de la préparation d'une directive émanant du Parlement européen et du Conseil, relative à certains aspects du commerce électronique sur le marché intérieur établit de la même manière que, « dans la mesure où elles sont concernées, les associations de consommateurs doivent être impliquées dans la rédaction et la mise en application des codes de conduite. De plus,

les utilisateurs doivent s'assurer de la parfaite transparence et accessibilité, de ces derniers tout autant que de leur évaluation.⁴⁸

La protection « adéquate » ou comment un ordre étatique peut imposer avec souplesse des valeurs aux pays tiers dans la société globale de l'information

En vertu de l'article 25.1. de la directive 95/46/CE citée plus haut, « les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve des dispositions nationales, prises en application des autres dispositions de la présente directive, le pays tiers en question offre un niveau de protection adéquat ». Le principe est donc l'interdiction du transfert sauf à démontrer le caractère adéquat de la protection offerte dans le pays tiers.

La directive précise ensuite, en son article 25.2., que l'appréciation du caractère adéquat de la protection du pays tiers doit tenir compte de « toutes les circonstances relatives à un transfert ou à une catégorie de transferts » et en particulier de différents facteurs, dont certains sont fonction du transfert considéré, tels la nature des données, la finalité et la durée des traitements, les pays d'origine et de destination, et dont d'autres concernent le niveau de protection dans le pays tiers, comme « les règles générales du droit ou sectorielles en vigueur ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées ».

Le texte de l'article 25 suppose en particulier une approche fonctionnelle c'est-à-dire que la protection s'évalue tant par rapport aux risques d'atteinte à la protection des données, risques générés par le flux en question, que par rapport aux mesures spécifiques ou générales mises en place par le responsable des données dans le pays tiers pour pallier ces risques.

L'évaluation de ces mesures doit se faire sans *a priori* ; il ne peut être question d'imposer les mécanismes européens mis en place en application de la directive (pas d'impérialisme européen) mais bien

48. Proposition amendée, présentée par la Commission conformément à l'article 250 du Traité de la Communauté européenne, pour une directive émanant du Parlement européen et du Conseil sur certains aspects juridiques du commerce électronique, dans le marché intérieur (1999/c30/04), COM (1998) 586, 18.11.1998, *Journal officiel de la Communauté européenne* 30, 5., 2, 1999, p. 4.

d'apprécier dans quelle mesure les objectifs de protection poursuivis par la directive sont rencontrés, de façon originale ou non, par un pays tiers. En ce sens, la notion de protection adéquate ne représente en aucune manière un affaiblissement de la protection des données telles qu'organisées par la directive. En effet, la notion de protection adéquate induit la confrontation des exigences de protection de la directive avec les réponses données par les pays tiers. Il s'agit de rechercher s'il y a « similarité fonctionnelle ». La « similarité fonctionnelle » implique que l'on recherche non la transposition pure et simple des principes et systèmes de protection européens dans le pays tiers, mais bien la présence de tout élément remplissant les fonctions recherchées, même si lesdits éléments doivent être d'une nature différente de ceux que l'on connaît en Europe. Elle permet sans doute un meilleur respect des structures et des caractéristiques juridiques locales qu'un requis de protection équivalente, qui exige une similarité législative complète.

En particulier, à propos des instruments de protection mis en place dans le pays tiers, l'article 25 se réfère non seulement aux normes issues de l'autorité publique, qu'elles soient générales ou sectorielles, mais également aux codes de conduite, voire aux mesures techniques pourvu que ces instruments soient « respectés ». Ainsi, la personne chargée d'évaluer la protection étrangère sera plus attentive à l'« effectivité » d'un instrument qu'à sa nature : ce qui importe, c'est que la connaissance de l'instrument, même s'il s'agit d'une simple *company privacy policy*, soit largement répandue parmi les personnes concernées et les responsables des fichiers ; de même, on sera attentif à la possibilité d'un recours des particuliers à l'encontre des responsables de fichiers en cas de non-respect des instruments en question. Enfin, on évaluera soigneusement la qualité de l'autorité en charge du recours, son accessibilité et la transparence de son fonctionnement⁴⁹.

À propos des conditions de l'autoréglementation

En conclusion, que tirer de ces deux dispositions de la directive « Protection des données », comme enseignement tant sur la valeur des normes privées que sur la relation ou la synergie entre normes privées et étatiques ?

Premièrement, la norme privée est d'autant mieux acceptée qu'elle est définie dans le cadre de principes ou standards fixés par

49. Voir Groupe de protection, 1998.

la norme étatique. De tels standards permettent en effet d'évaluer la conformité du contenu de la norme privée aux attentes sociétales mais donnent également à la norme privée une effectivité plus grande.

Deuxièmement, la norme privée peut être reçue comme « adéquate » à une norme étatique, si la procédure de sa création répond à certaines exigences de légitimité, d'abord dans la mesure où cette procédure a permis l'expression et la prise en considération des intérêts multiples des différents acteurs concernés par les opérations en cause ; ensuite, si la norme est transparente ; enfin et surtout, si l'effectivité de la norme est réelle, c'est-à-dire que des sanctions efficaces et proportionnées sont énoncées par une autorité dotée de pouvoirs d'investigation, agissant indépendamment des acteurs concernés, facilement accessible et dont le fonctionnement est transparent (par exemple à travers un rapport public d'activités ou la publication des décisions).

2.2.3. Conclusions

La norme étatique : une intervention nécessaire

À propos des sources étatiques, on s'interroge : à quoi sert-il que le législateur national légifère au moment où, comme nous l'avons montré, d'une part, le caractère international et ouvert du réseau, et, d'autre part, l'impossibilité de maîtriser les données spatio-temporelles des échanges conduisent à constater l'impuissance des États nationaux lors de l'application effective de la norme qu'ils se sont données ? L'émotion créée en janvier 1996 par l'intervention d'un parquet allemand ayant réclamé des fournisseurs d'accès le filtrage de messages pornographiques démontre cependant que même si le droit étatique ne dispose pas, en la matière, d'une efficacité complète, il peut néanmoins provoquer de la part des acteurs privés la mise en place, au sein du réseau, de solutions autoréglementaires certes non totalement mais partiellement satisfaisantes. Ainsi, le droit étatique ne peut démissionner ; mais sans prétendre réglementer, de manière complète, le réseau, il se doit de rappeler les valeurs sociétales exprimées par les normes, ne fût-ce que pour provoquer les réflexes d'autorégulation appropriés et leur servir de base. Il est remarquable de constater que même au pays de l'autoréglementation reine – les États-Unis d'Amérique –, l'Administration joue un rôle décisif dans la promotion de celle-ci. Ainsi, M. Pitofsky, Président de la Federal Trade Commission déclarait en août 1998 devant le Congrès : « Sauf si l'industrie peut démontrer

qu'elle a développé et mis en œuvre des programmes d'autorégulation bien fondés et efficaces à la fin de l'année, une autorité gouvernementale additionnelle serait appropriée et nécessaire. » On sait que depuis, le Gouvernement américain a mis au point l'idée d'une « Global Alliance » destinée à protéger efficacement, par la voie d'une autoréglementation sous contrôle, la protection de la vie privée et ce notamment dans le contexte de ces discussions avec l'Union européenne dans le cadre de l'application par cette dernière du prescrit de l'article 25 de la directive.

De plus, la recherche au sein d'organisations supranationales ou internationales comme l'UNESCO de principes et de solutions communs, – comme par exemple en matière de protection des mineurs, ou des consommateurs, de signature,... – favorisera l'uniformisation des conduites des acteurs, voire la coopération (ne serait-elle que policière !) entre les États. À défaut d'un tel consensus, la prise de position d'une organisation supranationale comme l'Union Européenne peut constituer le point de départ d'une négociation internationale avec les autres pays chargés de trouver, sans doute par des moyens plus en rapport avec leur propre tradition juridique, une protection adéquate vis-à-vis des principes affirmés par la même Union Européenne.

Confronté au phénomène sociétaire révolutionnaire que représente l'Internet, notamment la dislocation des frontières de l'espace et du temps, le droit étatique, expression de la régulation sociale des comportements, est – et se doit d'être – présent. Le droit ne peut se contenter de déplorer la difficulté de son application et d'affirmer que l'espace virtuel est un espace sans droit. Au contraire, il doit trouver dans une expression normative plurielle la manière adéquate d'agir : dans toute la mesure du possible, il renverra, par l'application de principes généraux (éventuellement adaptés ou reformulés), à des « normativités » présentes dans le réseau : l'application des principes sous forme d'autorégulation, la standardisation technique,... Il puisera, le cas échéant, dans le contenu de cette réglementation interne au réseau, l'inspiration pour définir, si possible au plan international, des règles de loi. Sans doute, s'agit-il, selon l'expression de M. Vivant⁵⁰, d'un droit postmoderne ou, selon celle de J. Reidenberg⁵¹, d'un nouveau « *network governance paradigm* ».

50. M. Vivant, 1997.

51. J. Reidenberg, 1996.

Loin de consacrer la démission de l'État, ce « droit postmoderne », ce « paradigme » nouveau invite à créer de nouveaux modes de dialogue entre diverses normativités techniques, éthiques et réglementaires et, tâche plus difficile, des instances démocratiques capables de susciter ce dialogue et de la mettre au service de l'intérêt général.

D'une part, l'État n'abandonne pas la réglementation de l'Internet à la seule initiative des utilisateurs du réseau. En effet, nous avons vu qu'à défaut de réglementations spécifiques, le rappel des grands principes de droit suggère l'adoption de règles par les acteurs et conduit à des développements techniques heureux.

D'autre part, on souligne l'ardente obligation de l'État d'intervenir au moment où, selon nous, délaisser l'Internet et se retirer de sa réglementation à tel point qu'il n'en fixe même plus le cadre général, parce que, notamment, l'ordre public, les libertés fondamentales et d'autres valeurs de base sont en jeu.

Le partage précis du travail entre l'élaboration de droits étatiques ou supranationaux et les initiatives des utilisateurs de l'Internet reste à définir. Il sera sans doute dynamique et devra permettre aux utilisateurs de faire preuve d'une certaine créativité dans la mise en œuvre du cadre avancé par le droit étatique.

De la valeur de l'autoréglementation et de ses limites

Cela dit, il ne peut être question de rejeter l'autoréglementation comme source normative au plein sens du terme. Comme conclut F. Osman : « Que l'on veuille y voir uniquement « une affaire de moment et de contexte », ou la preuve de ce que le droit subit « progressivement l'attraction et le joug des faits » économiques qui le dominent et dont il est devenu tributaire », un tel phénomène ne peut que susciter de l'intérêt pour le juriste à qui l'on a enseigné que la sanction fait partie du rouage de la règle de droit. Aussi est-ce tout naturellement qu'il est tenté de la rechercher partout, y compris dans le droit « mou ». Et si le critère de la sanction comme caractéristique de la règle de droit est un faux critère, et ce, en dépit des tentatives doctrinales pour le renouveler, c'est sans doute que l'effectivité des règles de conduite sociale, qu'elles « règlent ou régulent », ne réside pas nécessairement dans l'adhésion dont elles sont l'objet par le corps social destinataire. »⁵²

Que cette réflexion adressée aux sources normatives privées de la « *lex mercatoria* » soit également valable en matière de « *lex electronica* », certes mais elle ne peut avoir la même portée et, sans doute, cela justifie-t-il une intervention plus résolue du droit étatique. Premièrement, le milieu des internautes, sauf dans le contexte de *news group* ou dans certains milieux comme l'université ou le commerce entre marchands, est loin de présenter désormais la même homogénéité que celle des professionnels. Deuxièmement, là où la « *lex mercatoria* » ne règle que des questions économiques, c'est de culture, de valeurs et de libertés que traite la « *lex electronica* ».

Il apparaît dès lors que l'autoréglementation doit être contrôlée. Certes, elle peut présenter l'expression spontanée d'une communauté réelle mais ce sera rarement le cas. Aussi le droit étatique se doit-il de fixer au moins les standards à partir desquels se déclineront l'autoréglementation et les autres techniques normatives et veiller à ce que les mécanismes de mise au point de ces techniques de réglementation et l'application du contenu de ces normes privées soient transparentes et prennent en compte l'intérêt des divers acteurs.

3. LE RÔLE DE L'ÉTAT ET LA DÉFENSE DE VALEURS

Des rôles de l'État

Traditionnellement, le rôle de l'État est défini de manière triple : réglementer, stimuler et produire. La fonction de production s'entend du développement de produits et services par l'État. En matière de société de l'information, cette fonction tend à s'amenuiser tant les vertus de la concurrence et les besoins financiers de l'État ont conduit ce dernier à se séparer de ses entités productrices. C'est notamment le cas dans le secteur des télécoms où l'État exerçait autrefois son monopole mais, également, en matière d'exploitation de services télématiques administratifs (par exemple la gestion d'une banque de données multimédia en matière de cadastre) où l'État recourt largement à l'externalisation (*outsourcing*).

La fonction de stimulation ou de catalyse peut s'exercer de manière diverse. Si une réglementation adéquate – y compris fiscale – est un levier utile pour le développement de biens et services informationnels, on soulignera que la transformation des processus au sein de l'Administration ou entre Administrations et administrés par l'intégration des technologies de l'information et de la communication peut induire l'adoption par les administrés de ces mêmes technologies. Ainsi, tous les programmes nationaux relatifs

52. F. Osman, 1995, p. 531.

à la Société de l'Information mentionnent la nécessité d'un « *reeengineering* » de la fonction publique et on sait que l'utilisation électronique de formulaires administratifs comme ceux de la fiscalité indirecte amèneront en aval les entreprises à exiger de leurs partenaires des facteurs électroniques.

La première fonction, celle de réglementation, presse l'État d'épouser la cause des libertés. En effet, la première partie de notre article insistait sur la complexité des débats provoqués par l'utilisation des technologies de l'information et de la communication, et témoignait de la récurrence et de l'omniprésence de la question des libertés.

Nos réflexions partent en effet du constat que l'intervention de plus en plus prégnante d'opérateurs économiques, soutenus en leur action par les développements récents de la sécurisation des messages, modifie radicalement le paysage. Comme dit ci-dessus, l'Internet quitte rapidement le monde de la « foire aux idées » qui caractérisait les échanges de la communauté scientifique où il est, pour entrer dans le monde de la « foire commerciale ». Ainsi, deux mondes semblent actuellement coexister au sein de l'Internet :

- le premier étant le cyberspace, proche de la « foire aux idées », où la technologie apparaît, d'une part, comme le mode d'expression – certains ajouteraient « libre » – de tous et de chacun, expression d'autant plus libre que l'auteur d'un message décide ou non de s'identifier, choisit les correspondants avec qui ils souhaitent entrer en dialogue et, d'autre part, comme le mode d'accès aux libres créations d'autrui où qu'elles se trouvent dans le monde entier ;

- le second étant le « *superhighway* », proche de la « foire commerciale », où la technologie apparaît comme l'outil extraordinaire au service du marché, lui permettant d'améliorer les circuits de production de l'information mais surtout d'en contrôler la distribution. Les services électroniques de gestion des œuvres et la création de centres de certification des messages (voir *supra*, p. 214 et sp.) s'inscrivent bien dans cette deuxième optique ⁵³.

En d'autres termes, le développement de l'Internet oscille entre deux mondes : celui des libertés sans contrôle et celui fondé sur les lois du marché et sur les règles de la propriété ⁵⁴. C'est en tenant compte de cette évolution que nous affirmons le rôle essentiel du droit et de la fonction réglementaire pour le maintien d'une société libre.

La fonction de réglementation s'entend, d'une part, de la fixation de manière générale des règles du jeu globales (par exemple le droit de la concurrence) ou spécifiques à un secteur (par exemple le droit de l'audiovisuel), règles du jeu valables pour une société donnée et, d'autre part, de l'application de ces règles du jeu par des « organes nouveaux de réglementation », ces « autorités administratives indépendantes » dont nous avons déjà signalé l'existence et la multiplication (voir *supra*, p. 194).

Des valeurs comme celles de « libertés » et de non-discrimination

Débarrassé de sa fonction de production, l'État concentrera son rôle autour de la défense, mieux, de la promotion de certaines valeurs.

Même des questions aussi privatistes que celle du droit des contrats mettent désormais en jeu des questions de libertés et de non-discrimination. C'est avec l'apparition des « notaires électroniques », le droit de chacun à la signature électronique. C'est la nécessité de développer pour des raisons de protection de la vie privée, le droit de l'utilisateur avoir accès à des techniques d'anonymisation de la transaction vis-à-vis de certains intervenants dans la transmission, voire vis-à-vis également du destinataire. C'est, en droit de la propriété intellectuelle, à travers l'idée de licences obligatoires, la volonté de ne pas réserver aux seuls nantis l'accès à l'information mais de le garantir à tous afin d'éviter une société duale. Enfin, c'est l'omniprésence du principe de la liberté d'expression dont la jurisprudence de la Cour européenne des droits de l'homme rappelle qu'elle ne peut être limitée par d'autres intérêts supérieurs ou libertés fondamentales que dans la mesure strictement nécessaire à l'exercice de ces intérêts ou libertés, ce qui amènera l'État non seulement à éviter un excès de réglementation mais également à veiller à ce que l'autoréglementation ne devienne pas un outil de censure bien plus efficace et dangereux que la surveillance policière.

Au-delà, l'État cherchera, d'une part, par une politique dite de service universel à ce que chaque citoyen ait la possibilité d'accéder aux bénéfices de cette société informationnelle et, d'autre part, à mettre en place les instruments d'une meilleure participation des citoyens à la définition de la *res publica*, en évitant les pièges de ce que certains appellent la « démocratie électronique ». Ce sont ces deux derniers points que nous allons développer.

53. C. Lamouline et Y. Pouillet, 1997, p. 112-113.

54. E. Mackaay, 1996.

3.1. Au-delà du service universel des télécommunications : le service universel dans la société de l'information

Du service universel des télécommunications

L'idée essentielle de non-propos est de démontrer que la citoyenneté dans la société de l'information exige plus que le service universel des télécommunications tel que récemment défini par l'Union Européenne à la suite des États-Unis d'Amérique. La notion est définie à la fois comme un service qui est à la fois universel (lequel suppose un accès pour tous à un prix abordable), égal (impliquant un accès non discriminatoire et en tout cas indépendant de la situation géographique) et continu, c'est-à-dire caractérisé par une fourniture ininterrompue dans une qualité donnée.

La notion de service universel a le mérite qu'elle permet, tout en respectant le dynamisme d'un marché concurrentiel et en refusant dès lors le monopole étatique, de mettre l'accent sur la manière dont le développement des nouvelles technologies doit permettre à chacun de mieux participer à la société et à la définition du vouloir vivre ensemble. À cet égard, l'extension de la notion de service universel est évolutive dans la mesure où elle prend en compte le développement technologique et sa diffusion croissante au sein de la société.

Le service universel s'entend d'abord comme l'accès à des techniques de communication : l'accès au réseau, ou au service téléphonique aujourd'hui ; l'accès au courrier électronique, aux autoroutes de l'information demain. Seul, ce service universel des télécommunications est jusqu'à présent pris en considération par les textes européens.

Un second aspect du service universel des télécommunications déjà présent dans certains textes européens et privilégié par le texte légal belge du 17 décembre 1997 est de permettre, en favorisant la connexion des écoles et des bibliothèques publiques, l'accès de tous à la culture technique.

Au service universel dans la société de l'information

La « National Information Infrastructure Policy » (1993) de Clinton et Gore apporte à la notion de service universel une dimension révolutionnaire, sans que pour autant ne soit modifiée sa définition. La notion de service universel est chaque jour plus vitale, et apparaît comme le moyen de lutter contre les discriminations sociales.

Récemment, cette volonté politique a été consacrée par le Telecommunications Act de 1996 dont la section 254 établit les princi-

pes du service universel, en définit l'extension et enfin, met sur pied une procédure de révision périodique du contenu ⁵⁵.

Les conséquences d'une telle approche positive, qui fonde le développement d'une société de l'information sur l'épanouissement de nos libertés, mettent en évidence l'importance et la nécessité d'une redéfinition du service universel, entendu non plus comme le seul accès aux moyens techniques de communication (l'infrastructure et le service de transport de la voix), mais également comme l'exigence de création et de mise à disposition pourrait s'introduire dans la notion de service universel, au vu de ce qui est considéré comme « essentiel » et « vital » pour assurer la participation des citoyens dans une société démocratique. Il s'agit, selon l'expression américaine propre à la définition de la politique de la National Information Infrastructure, de veiller à ne pas introduire de discrimination entre ceux qui détiennent la connaissance et ceux qui ne la détiennent pas (les « informations haves » et les « informations haves not »). Comme le proclame le groupe d'experts réuni à l'UNESCO en 1998, « le droit de communiquer est un droit fondamental de l'être humain » (1^{er} principe) et « de ce fait tout citoyen doit avoir le droit de participer effectivement à la société de l'information » (2^e principe), ce qui implique (3^e principe) « que les États devraient promouvoir des services universels où, dans la mesure du possible et compte tenu des différences de situation et de ressources selon les pays et les régions, les nouveaux médias seraient accessibles localement à tous, sans discrimination et indépendamment du lieu ».

Ainsi, tout en reconnaissant les expressions multiples et différenciées de ce droit selon les niveaux de développement de chaque pays, il s'agit de ne pas se contenter d'un accès, selon les prix abordables et de manière non discriminatoire, à un réseau ni même à un service envisagé sous l'angle purement technique, mais d'assurer l'accès à des contenus informationnels.

On connaît les exemples célèbres de la politique américaine : l'accès à la formation, aux soins de santé,... Il s'agit de mettre à la disposition de tous et de chacun, via les télécommunications et selon des modalités diverses en fonction du service considérée, certains services d'intérêt général afin d'éviter une société à deux vitesses.

Divers rapports nationaux (canadien, français, néerlandais, danois,...) insistent sur la nécessité d'une politique volontariste

55. F. van der Mensbrugghe, 1998.

d'éducation à l'utilisation des technologies dans les établissements scolaires secondaires, voire de premier degré. Au-delà de la connexion des écoles aux infrastructures, l'utilisation des technologies interactives peut être un outil d'aide précieux à l'enseignement, en même temps qu'elle favorise la maîtrise dudit outil par les étudiants. Une telle éducation devrait également comporter des enseignements de lecture de l'image, qu'elle soit publicitaire, d'information générale ou autre, afin de permettre au futur utilisateur des nouveaux médias de pouvoir « décoder » les messages véhiculés par les réseaux. Comme le note le groupe d'experts réuni par l'UNESCO, « toute personne devrait avoir le droit de recevoir l'éducation nécessaire pour lire, écrire et travailler dans le cyberespace. Des initiatives spéciales devraient être prises pour informer les parents, les enfants, les enseignants et d'autres utilisateurs de l'Internet des incidences de leur participation au cyberespace et de la façon d'utiliser au mieux les possibilités offertes par ce nouveau média » (4^e principe).

On ajoute l'intérêt de la création de « centres d'information » ouverts à tous, qui, par ailleurs, pourraient être localisés dans des bibliothèques publiques. Des expériences locales témoignent du double intérêt de ces centres : d'une part, ils permettent à certaines populations écartées de l'accès aux services d'information pour des raisons financières de trouver ainsi un accès à des coûts raisonnables ; d'autre part, ils stimulent, le cas échéant, une communication orale directe entre plusieurs personnes physiques réunies et écartent le risque d'une technologie « isolante » où seule la communication virtuelle et individualiste est proposée.

En matière médicale, on notera le développement du concept de Public Health Universal Service, soit l'obligation positive faite à l'administration de mettre sur pied, tantôt des services *on-line* d'assistance à remplir des formulaires administratifs, tantôt des services d'information en matière médicale, statistique ou autre, obligation dont découle le devoir de l'État d'apporter des subsides à certains établissements, en particulier d'enseignement universitaire, pour avoir accès à de telles données, voire pour les diffuser.

Sous ce concept de service universel de santé public, est également comprise la mise sur pied d'infrastructures de communication à haut débit entre, d'une part, des hôpitaux situés dans des régions de faible population et disposant dès lors de personnel peu qualifié et, d'autre part, des hôpitaux qui, du fait de leur localisation ou de leur statut universitaire, disposent de ce personnel qualifié. De tels réseaux de communication permettent d'améliorer le service public de la santé.

Cet exemple peut être étendu à d'autres secteurs tant il est vrai que dans bien des secteurs de la vie administrative, les technologies de l'information et de la communication peuvent favoriser l'accès au service public. Ainsi, que ce soit en matière sociale ou fiscale, de permis de bâtir, la création de services *on-line* d'assistance pour remplir des formulaires administratifs ou envoyer des formulaires ; dans le domaine du service public de la justice, des systèmes électroniques de certification de messages pour l'enregistrement de plaintes, le dépôt ou l'échange de conclusions.

En bref, c'est tout le fonctionnement de l'administration et de son service qui peut être revu dans la perspective du développement des technologies de l'information et de la communication.

Cette transformation du service rendu par les administrations trouve un fondement légal dans la loi du changement, principe clé du service public et dans les lois d'accès aux documents administratifs. Ce droit doit désormais être conçu en particulier dans un environnement électronique comme le moyen non seulement d'assurer le droit à l'information du citoyen vis-à-vis de son administration (voir à ce propos, *infra*, § 3.2, NTIC) mais, de manière plus volontariste, de rendre un meilleur service aux citoyens ⁵⁶.

De l'intérêt d'un concept large

En conclusion, l'intérêt du concept de service universel est multiple. Premièrement, on rappelle l'objectif social poursuivi par les tenants de ce concept : il s'agit d'éviter la dualisation de la société. Deuxièmement, la définition du contenu nécessairement évolutif du service universel nécessite la discussion de toutes les parties intéressées au sein de forums avant toute décision de l'autorité publique et est ainsi un gage de participation de tous à la définition de la Société de l'information de demain. Troisièmement, le concept de service universel, de préférence à celui du service public, met l'accent sur le fait d'une possible participation du privé à l'une ou à l'autre des

56. Un colloque, intitulé « L'information juridique : contenu, accessibilité et circulation. Défis politiques, juridiques, économiques et techniques » (Paris 22-23 octobre 1998), a été organisé par l'Association française pour le développement de l'informatique juridique (ADIJ) sur l'analyse des initiatives récentes prises par des gouvernements de certains États (Belgique, Canada, France, Pays-Bas, États-Unis) sur la diffusion de documents juridiques. Les textes des différentes interventions sont accessibles sur le site web de l'ADIJ : <http://www.adij.assoc.fr>.

tâches de mise sur pied ou de diffusion de chaque service jugé d'intérêt général. Cette collaboration de l'Administration et du privé peut apparaître comme une meilleure garantie d'efficacité du service, à condition que ne se substitue point à un monopole public, un monopole privé et que des garanties existent à cet effet (règles de concurrence, de marchés publics,...).

3.2. La démocratie électronique : du mythe à la réalité ⁵⁷

NTIC et démocratie : un dialogue à facettes multiples

Les nouvelles technologies de l'information et de la communication permettent également de promouvoir la liberté d'expression et d'information et, de manière plus large, la démocratie : elles facilitent l'accès des citoyens à l'information publique ; elles offrent aux citoyens la possibilité d'être consultés ou d'intervenir de manière plus directe dans le processus de décision ; elles peuvent constituer un danger lorsqu'elles sont utilisées à mauvais escient par les partis politiques ou par des lobbys soucieux de peser sur la décision politique.

Autour de ces thèmes, deux questions seront successivement examinées.

Premièrement, la réflexion sur les autoroutes de l'information stimule une revitalisation des lois d'accès aux documents administratifs (« Freedom of Information Acts »). Grâce à la transparence de l'action administrative que ces lois assurent, elles apparaissent comme la condition indispensable de l'expression libre et éclairée de chacun dans une société démocratique.

Deuxièmement, ces mêmes technologies offrent aux citoyens la possibilité d'être consultés, voir d'intervenir de manière plus directe dans tous les processus de décision, en particulier au niveau local. Cette conduite induit l'utilisation croissante par les partis politiques des possibilités offertes par les nouvelles technologies, utilisation qui suscite bien des espoirs mais également des craintes qui justifient la définition de certaines règles du jeu.

57. Nous reprenons ici certaines idées développées dans le chapitre III de l'ouvrage de C. Lamouline et Y. Pouillet, 1997.

3.2.1. De l'accès aux documents administratifs à l'accès électronique

Les fondements d'une législation

La liberté d'expression reconnue à l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales suppose, pour être effective, une obligation tant active que passive à charge de l'État, obligation d'informer tant sur l'action entreprise que sur celle à entreprendre. Le droit du public d'être informé, entendu non comme droit subjectif mais comme principe démocratique, trouve sa principale traduction dans la liberté d'information. Celle-ci, portant sur les relations entre l'administré et le pouvoir, prend un sens très particulier et signifie la faculté pour tous les citoyens de prendre connaissance des documents gouvernementaux ainsi que de l'information détenue par l'administration publique. La liberté d'information, instrument de la transparence des institutions publiques et administratives, offre par cette progression vers l'instauration d'une démocratie de participation le complément indispensable aux régimes actuels de démocratie représentative. Le débat public au sein du corps social, ne peut prendre place que sur la base de l'accès à l'information détenue par le secteur public. Cette assertion fondait déjà le principe même de la Recommandation du Conseil de l'Europe sur l'accès à l'information détenue par les autorités publiques, recommandation qui a trouvé son prolongement dans les multiples lois nationales dites de « Freedom of Information ». L'utilisation des technologies de l'information et de la communication (TIC) donne à ce droit d'accès des expressions voire une signification nouvelle.

L'accès électronique aux documents administratifs

Sous l'impulsion de la « National Information Infrastructure Policy » américaine, se sont mises en place un peu partout aux États-Unis, surtout au niveau local, des technologies simples qui, à partir, de guichets automatiques, permettent d'exercer les droits prévus par ces législations de manière plus efficace. Ainsi peut-on obtenir directement des informations et services (état civil, cadastre, service des impôts, sécurité sociale) de la part de municipalités et ce à partir de chez soi ou de guichets situés en divers points de la ville.

Il ne s'agit plus simplement d'assurer l'accès, voire la distribution électronique d'informations jugées essentielles, ainsi de bases de données gouvernementales statistiques, géographiques, démographiques, administratives, légales mais également de permettre un dialo-

que électronique interactif entre l'Administration et les citoyens. Ainsi, on peut concevoir que les citoyens puissent, grâce à l'interactivité des réseaux, interroger directement l'Administration sur des procédures qui les concernent et accomplir des démarches sans déplacement (un permis de bâtir, une inscription à un registre de commerce,...). Il s'agit donc d'assurer la possibilité d'un contrôle continu de l'action de l'Administration dans les dossiers concernant les citoyens.

En poussant plus loin le raisonnement, on peut se demander si le traitement des données administratives ne devrait pas être conçu de façon à ce que les citoyens puissent y accéder directement par leur propre terminal. Ces questions font l'objet de discussions aux États-Unis d'Amérique dans le cadre de la liberté d'accès à l'information électronique ; c'est seulement au Canada, au niveau fédéral, que la législation ouvre le droit à un « temps d'ordinateur » c'est-à-dire un droit pour les administrés d'utiliser certains programmes de l'Administration pour traiter des données administratives en vue de répondre à une demande directe d'accès.

Au travers de multiples développements et suggestions se lit la volonté d'une profonde modification du droit d'accès. Il ne s'agit plus simplement d'assurer le droit à l'information du citoyen vis-à-vis de son administration mais, de manière plus volontariste, de transformer, grâce aux technologies de l'information, cette administration devenue transparente en un meilleur service aux citoyens.

Ces nouvelles applications de la technologie de l'information et de la communication posent avec acuité le problème de l'accessibilité aux réseaux. En effet, le refus de la dualisation de la société entre les « *information haves* » et les « *have nots* » ne se justifie plus seulement par des considérations de justice sociale mais par une exigence démocratique qui requiert la possibilité pour tous d'accéder aux services administratifs. L'État se doit de lever les obstacles à l'accès aux nouveaux services proposés.

À cet égard, à la suite de Wellman et Gulia⁵⁸, on distinguera trois niveaux d'accessibilité : physique, économique, culturelle. L'accessibilité physique semble pouvoir être assurée de façon satisfaisante dans un avenir proche par une évolution et une diffusion spectaculaire des technologies. L'accessibilité économique peut être atteinte par la diminution continue des tarifs, la mise à disposition d'ordinateurs dans des lieux publics, voire la notion de service universel consacrée de manière extensive. Le véritable défi reste l'accessibilité culturelle ou

cognitive quand on pense que l'expression écrite se révèle difficile pour une partie minoritaire mais importante de la population. Faute de pouvoir assurer ces trois niveaux d'accessibilité, il est important que l'État maintienne les formes traditionnelles d'accès aux services administratifs (formulaires papier ; guichets physiques).

3.2.2. *L'amélioration de la participation des citoyens aux décisions politiques :*

Les « civic networkings », les villes virtuelles

L'interactivité des réseaux permet de concevoir ces derniers comme un outil de meilleur dialogue entre les citoyens, d'une part, les décideurs et les lobbies, d'autre part. Dès maintenant, l'Internet offre de nombreux « Bulletin Board Systems » où s'échangent des messages autour de questions d'intérêt général qu'elles soient locales, nationales ou internationales, thématiques ou non.

Le Professeur Rodota décrit comme suit l'expérience américaine à cet égard : Aux États-Unis d'Amérique, à côté de l'expérience Internet et d'autres grands réseaux télématiques, on compte de multiples expériences locales, dont la plupart sont gérées par des organisations privées de villes virtuelles (*civic networking*). Presqu'une centaine de villes américaines se sont dotées de Civic Networks opérationnels (réseaux d'informatique civique) ou de FreeNets (réseaux auxquels on peut accéder gratuitement ou à très bon marché) et, pour coordonner leur développement, elles se sont associées en un « réseau des réseaux », le National Public Telecomputing Network (NPTN) qui regroupe l'ensemble de ce qu'il est convenu d'appeler les « Digital cities ». Ces organisations ne prévoient pas seulement l'accès à Internet, mais elles relient en outre les citoyens à des bureaux publics, à des bibliothèques, à des archives, à des écoles, à des universités, à des centres de recherche, à des hôpitaux, à des entreprises. Le but principal de l'opération est d'offrir aux usagers une série de services qui concernent le gouvernement et l'activité législative, l'administration et la politique, outre les intérêts sociaux, sanitaires, éducatifs et économiques⁵⁹.

Ces services de consultation de la population devraient être organisés par les gouvernements de manière systématique à tous les échelons locaux, régionaux voire internationaux, et ce dans le respect des règles concernant la vie privée (*privacy*).

58. B. Wellman et M. Gulia, 1998.

59. S. Rodota, 1995.

Il s'agit d'une forme moderne d'organisation de « *public hearings* » qui peut utilement éclairer les décideurs, en les informant de points de vue soit individuels soit collectifs. Nous pensons que certaines règles devraient être suivies dans l'organisation de ces hearings, afin d'organiser la transparence de la procédure, dans son déclenchement et dans ses résultats, qui doivent pouvoir être accessibles tant à la majorité qu'à l'opposition.

Le référendum électronique

Ross Perot, candidat malchanceux à la Présidence des États-Unis, a contribué à rendre populaire le concept d'« *Electronic Town Halls* ». Il s'agit pour une autorité, en particulier mais non exclusivement, locale de développer des modes électroniques de décisions des électeurs. Le but, selon Ross Perot, était d'instaurer à côté de la démocratie représentative, une forme de démocratie directe, permettant des consultations politiques plus rapides et offrant au citoyen un mode de ré-appropriation de la *res publica*.

Certes, le référendum électronique favorise la démocratie directe. Il ne doit cependant être évalué non à l'aune de ses potentialités techniques mais selon ses implications sur nos systèmes politiques contemporains. Même sans se substituer aux décisions parlementaires⁶⁰, le référendum électronique présente des dangers et comporte cependant des risques de dérives, accentués par l'aspect *push button*. On connaît les risques de manipulation du public inhérents à ce type de procédé, lors du choix des problèmes à traiter par référendum et lors de la rédaction des questions soumises à la population. Mais il est à craindre que la technologie banalise ce type de consultation et que l'interactivité, par écran interposé, forme de *livingroom democracy*, prive le citoyen, par la garantie de l'isoloir, à la fois du recul nécessaire et du débat public utiles pour appréhender la portée de la question posée et pour y réagir⁶¹.

Sans doute, des règles éthiques et normatives devraient être édictées à ce propos. Ainsi, dans toutes les hypothèses, l'obligation d'indiquer clairement le but, les modalités, les conséquences et le responsable de l'organisation de la consultation opérée, l'interdiction d'enregistrer les données personnelles résultant du sondage ainsi effectué devraient être affirmées ; dans les cas où la consulta-

tion électronique est organisée par une autorité publique, les obligations suivantes devraient être imposées :

- a) obligation de soumettre préalablement le questionnaire à une discussion au sein des organes de démocratie représentative ; le cas échéant, obligation de rendre accessible les remarques opérées par chaque courant d'opinion sur le questionnaire soumis à la consultation ;
- b) obligation de publier préalablement le questionnaire et lesdites réflexions par voie électronique et par d'autres voies ;
- c) obligation de prévoir d'autres modalités de consultation que la seule voie électronique ;
- d) obligation de publier de manière complète les résultats du référendum (en particulier nombre de personnes ayant répondu, modalités d'interrogation,...) ;
- e) interdiction de fonder une décision sur les seuls résultats d'une consultation électronique.

L'utilisation par les partis et les hommes politiques des technologies de l'information et de la communication

Quelques exemples récents témoignent de l'importance prise par les médias électroniques dans la diffusion des messages politiques des partis. Le cas « Berlusconi » est souvent cité mais, au-delà, c'est progressivement chaque parti, voire chaque homme politique, qui se dote de serveurs électroniques et organise la communication d'informations, voire le débat sur tel ou tel thème, via des systèmes électroniques.

Certains auteurs n'hésitent pas à dénoncer les dangers de cette médiatisation de la politique qui court-circuite les formes traditionnelles d'apprentissage politique, conduit à une simplification à outrance du message en quelques slogans populistes et caricaturaux. Surtout, l'utilisation des médias entraîne une formation à l'opinion politique en dehors des lieux communautaires (*meetings électoraux*,...) où, traditionnellement, cette opinion se forgeait.

Le fait que de telles dérives puissent exister, exige que nos programmes éducatifs scolaires contiennent désormais des cours d'analyse critique des messages véhiculés par les nouveaux médias. Au-delà, il importe que l'accès aux nouveaux médias soit garanti à chaque courant d'opinion et que, de la même manière que pour les messages électoraux des partis dans les médias classiques (papier, audiovisuel), des règles similaires soient prises pour les nouveaux médias. Ainsi, on songe aux obligations suivant lesquelles la nature

60. P. Lévy, 119.

61. S. Rodota, 1997.

de tels messages et l'auteur de ceux-ci soient clairement identifiés, que le citoyen puisse accéder, via un serveur unique, à l'ensemble des messages électoraux des différents partis et que l'anonymat même dans la consultation de ces programmes soit garanti, à la demande de l'utilisateur.

De nombreuses règles électorales (celles relatives à l'organisation des campagnes électorales, à l'interdiction de diffamations et au droit de réponse, au contrôle strict de la publicité électorale, à l'interdiction de publication des sondages, à la durée de la campagne) trouvent difficilement application en dehors des médias traditionnels et « invitent à une certaine révision de nos schémas de pensée (réglementaire) habituels ». Sinon le droit de la communication audiovisuelle perdra toute cohérence pour éclater en des droits spécifiques attachés à chaque média et les mécanismes de la démocratie électronique seront faussés par les capacités de la technique.

4. CONCLUSIONS

Les rôles du droit

Le rôle du droit face aux développements de la société de l'information est multiple.

Sa première mission est certes celle de se remettre en cause. Il ne s'agit pas là, bien au contraire, de céder à la tentation de la modernité et, par une écriture autant hâtive que brouillonne, de consacrer l'originalité du donné technologique. Bien au contraire, l'invitation à « relire » le droit exige un moment de recul qui permettra à la fois l'approfondissement des valeurs et des équilibres inscrits au cœur des concepts traditionnels et l'attention aux nouveaux enjeux.

Pour résoudre ces nouveaux enjeux, le juriste – c'est sa seconde mission – se doit d'être un médiateur, entre les multiples intérêts parfois contradictoires, souvent conflictuels que génèrent vis-à-vis de différentes catégories d'acteurs l'utilisation de ces technologies.

Le droit se doit donc, plutôt que de figer des arbitrages remis en cause, à peine l'encre séchée, de mettre en place des organes au sein desquels pourra être appréciée de manière transparente combien l'évolution modifie les équilibres fragiles à peine définis.

Un tel constat plaide pour un droit plus procédural que de contenu. Il s'agit de mettre en place des lieux ouverts et transparents au sein desquels la discussion pourra avoir lieu.

Ces lieux sont divers. En dehors des acteurs publics, la norme peut émaner de cercles privés. Le droit se doit de reconnaître de telles normes et de multiplier les dialogues entre auteurs publics et privés, construire cette « internormativité » qui caractérise la réglementation du secteur des technologies de l'information et de la communication. L'État rappellera cependant vis-à-vis des sources privées l'exigence d'une légitimité de ses auteurs et de son contenu, légitimité qui ne peut naître que de la transparence de la discussion ou du moins de la prise en compte des intérêts de chaque acteur concerné par la question débattue.

Le même souci de souplesse et de médiation entre acteurs aux intérêts divers, poussera le droit à multiplier les « autorités administratives indépendantes », à leur donner la même autonomie créatrice mais à exiger d'elles un fonctionnement transparent et ouvert.

Enfin, la volonté de définir un vouloir-vivre ensemble devrait conduire à la création d'un lieu de réflexion nationale, lieu de veille technologique, de concentration et de définition de politiques globales où se forgera au terme de débats publics les grandes options de notre société non seulement informationnelle mais démocratique.

BIBLIOGRAPHIE

- Antoine M., Gobert D., « Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification », *Revue générale de droit civil*, p. 285-310, 1998.
- Boulanger M.-H. et al., « La protection des données à caractère personnel en droit communautaire », *Journal des tribunaux de droit européen*, p. 121-127, 145-155, 173-179, 1997.
- Brouir J.N., Martens P., In : *Liberté, droits et réseaux dans la société de l'information*. Paris-Bruxelles Bruilant, LGDJ, 1996.
- Cerf V., *Guidelines for Conduct on and Use of Internet*, 14 août 1994, disponible à : <http://info.isoc.org:80/policy/conduct/cerf-Aug-draft/html>.
- Couret A., Igalens J., Penan H., *La certification*. Paris, PUF, collection Que sais-je ?, 1995.
- Davio E., « Questions de certification, signature et cryptographie, Internet face au droit », *Cahiers du Centre de recherches informatiques et droit*, n° 12, p. 65-86, 1997.

- Decoopman N., « Droit et déontologie : contribution à l'étude des modes de régulation », In : *Les usages sociaux du droit*, p. 87-105, Paris, PUF, 1989.
- Dinant J-M., « Les traitements invisibles sur Internet », *Cahiers du Centre de recherches informatiques et droit*, 1997.
- . Using PICS as an Enhancing Privacy Technology, [http :/ www.droit.fundp.ac.be/crid/eclip/pics.html](http://www.droit.fundp.ac.be/crid/eclip/pics.html), 1998.
- . « Communication ou A-Communication ? L'électronisation du commerce », *Revue générale*, n° 3, p. 39-47, 1999.
- Dunne R., « Deterring unauthorized access to computers : controlling behavior in cyberspace through a contract law paradigm », *Jurimetrics Journal*, n° 35, p. 11 et sq., 1994.
- Dussollier S., « Electrifying the fence : the legal protection of technological measures for protecting copyright », *European Intellectual Property Review*, p. 285-97, 1999.
- Electronic Frontier Foundation (EFF). General Information about the Electronic Frontier Foundation, Washington DC, [http :/ www.eff.org/EFFdocs/about_eff.html #INTRO](http://www.eff.org/EFFdocs/about_eff.html#INTRO), 1995.
- Frydman B., *Quel droit pour l'Internet, Internet sous le regard du droit*, Bruxelles, Ed. Jeune Barreau, 1997, p. 295 et sq.
- Grossman L.K. *The Electronic Republic. Reshaping Democracy in the Information Age*, 20th Century Fund Book, 1995.
- Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, Document de travail, XVD/5025/98, WP 12. Transferts de données à caractère personnel vers des pays tiers : Application des articles 25 et 26 de la directive relative à la protection des données à caractère personnel, adopté par le groupe de travail le 24 juillet 1998.
- Gutwirth S., *Waarheidsaanspraken in Recht en Wetenschappen*, Bruxelles-Anvers, Maklu, 1993.
- Hardy T.I., « The Proper Legal Regime for Cyberspace », *University of Pittsburg Law Review*. (Pittsburg), n° 55, p. 993-1055, 1994.
- Johnston D., Post D., *Laws and Borders : The Rise of Law in Cyberspace*, http://www.cli.org/X0025_LBFIN.html, 1996.
- Katsh E., *The Online Omsbut Office : Adapting Dispute Resolution to Cyberspace*, <http://www.law.vill.edu/ncair/disres/katsh.htm>
- Lamouline C., Pouillet Y., *Des autoroutes de l'information à la démocratie électronique*, (Report to the Council of Europe) Bruxelles, Nemesis Bruylant, 1997.

- Lavenue J.-J., « Cyberspace et droit international : pour un nouveau jus communicationis », *Revue de la recherche juridique - droit prospectif*, p. 811-844, 1996.
- Levy P., *Cyberculture : Rapport au Conseil de l'Europe*, Paris, O. Jacob, p. 228 et sq, 1997.
- Liberté, droits et réseaux dans la société de l'information*, (Voir notamment articles de J.-N. Brouir et P. Martens.) Paris/Bruxelles, LGDJ, 1996.
- Longworth E., *Possibilities of a Legal Framework for Cyberspace - including a New Zealand Perspective*, Réunion d'experts de l'UNESCO pour la région Asie-Pacifique sur un cadre général pour le cyberspace (République de Corée, 8-10 septembre 1998).
- Louveaux S., Pouillet Y., Salaun A., *User Protection in the Cyberspace : some Recommendations*, <http://www.jura.uni-muenster.de/eclip>, 1999.
- Mackay, *Lawyering and Litigating in Cyberspace. Address to the Eleventh Colloquium on Legal Data Processing in Europe*, 4 octobre 1993.
- Montero E., « Les responsabilités liées à la diffusion d'informations illicites ou inexactes sur Internet : Internet face au droit », *Cahiers du Centre de recherches informatiques et droit*, n° 12, p. 111-136, 1997.
- . *La responsabilité du fait des informations accessibles en ligne*, Namur, PUN, 1998.
- Osman F., « Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc. : réflexions sur la dégradation des sources privées du droit », *Revue trimestrielle de droit civil*, p. 509-31, 1995.
- Perritt H.H. Jr, *The Electronic Agency and the Traditional Paradigms of Administrative Law*, *Administrative Law Review*, vol. 44, p. 79-105, 1992.
- . « Dispute Resolution in Electronic Networks Communities », *Villanova Law Review*, p. 349-401, 1993.
- . « Jurisdiction in Cyberspace : the role of intermediaries », In : *Symposium on Information, National Policies and International Infrastructure*, Harvard, 28-30 janvier, <http://www.law.vill.edu/harvard/article/harv96k.htm>, 1996.
- Post D., *Anarchy, State and the Internet : an Essay on Law-making in Cyberspace*, J. Online L art 3. <http://www.law.cornell.edu/jol/post.html>, 1995.

- Poullet Y., « Le droit de l'informatique existe-t-il ? », In : *Droit de l'informatique : enjeux-nouvelles responsabilités*, Bruxelles, Conférence du Jeune Barreau, p. 1-43, 1993.
- Poullet Y., « Libertés fondamentales et société de l'information », *Revue générale, Communication ou a-communication*, numéro spécial, p. 21-28, mars 1999.
- Poullet Y., Queck R., « Le droit face à Internet, Internet face au droit », *Cahiers du Centre de recherches informatiques et droit*, n° 12, p. 231-249, 1997.
- Poullet Y., Havelange B., *Preparation of a Methodology for Evaluating the Adequacy of the Level of Protection of Individuals with Regard to the Processing of Personal Data*, Office for Official Publication of the European Communities, ISBN 92-828-4304-1. XV D/5047/98, Annex to Annual Report 1998.
- Poullet Y., Royen J., Rapport de l'atelier Commerce électronique : vers la confiance, AGORA, n° 98, 16 décembre 1998.
- Rapport de la réunion d'experts sur le droit du cyberspace, Monte-Carlo, 29-30 septembre 1998, Doc. CII/USP/ECY/99/01 du 22.02.99.
- Reidenberg J., « Governing Networks and Cyberspace Rule-making », *Emory Law Journal*, p. 911, 1996.
- , « Governing networks and cyberspace rule-making », In : *Symposium on Information, National Policies and International Infrastructure*, Harvard, 28-30 janvier, <http://ksgwww.harvard.edu/~itbspp/reidpap2.htm>, 1996.
- , « Lex informatica : the formulation of information policy rules through technology », *Texas Law Review*, vol. 3, p. 553 et sq., février 1998.
- Rigaux F., *Droit public et droit privé dans les relations internationales*, Paris, Pedone, 1977.
- , « Le droit au singulier et au pluriel », *Revue interdisciplinaire d'études juridiques*, n° 9, p. 45 et sq., 1997.
- Rinaldi A., *The Net : User Guidelines and Netiquette*. <http://www.fau.edu/rinaldi/net/index.html>, 1995.
- Rodota S., Démocratie électronique, Rapport général par le Conseil de l'Europe. *Séminaire sur la demande électronique*, Paris, Sénat, Palais du Luxembourg, 23-24 mars 1995.
- , *Technopolitica : la democrazia e le nuove tecnologie della comunicazione*, Rome, Sagitari Laterza, 1997.
- Romano S., *L'ordre juridique*, Paris, Dalloz, 1975.

- Samuelson P., *Technological Protection for Copyright Works*, <http://www.sims.berkeley.edu/~pam/courses/cyberlaw/docs/techpro.html>, 1996.
- Schlachter E., *The Intellectual Property Renaissance in Cyberspace : why Copyright Law Could Be Unimportant on the Internet*. <http://www.law.berkeley.edu/journals/btlj/articles/12-1/schlachter.html>
- Sturman C., Technische normen en het recht, Beschouwingen, over de interactie tussen het recht en technische normalisatie op het terrein van informatietechnologie en telecommunicatie. *Informatica en Recht*, n° 17, Vrije Universiteit Amsterdam, Kluwer, 1995.
- Trudel P., « Les effets juridiques de l'autoréglementation », *Revue de droit de l'Université de Sherbrooke*, n° 19, p. 247-286, 1988-1989.
- , « Les effets juridiques de l'autoréglementation », *Revue de droit de l'Université de Sherbrooke*, vol. 19, p. 247-286, 1988-89.
- , « Le cyberspace : réseaux constituants et réseau de réseaux », In : J. Frémont et J.-P. Ducasse (dir. publ.), *Les autoroutes de l'information : enjeux et défis*, Montréal, Les chemins de la recherche, 1996, p. 137-59. Actes du Colloque tenu dans le cadre des Huitièmes entretiens Centre Jacques Cartier, Rhône-Alpes, 5-8 décembre 1995.
- Trudel P. et al., *Droit du cyberspace*, Université de Montréal, Thémis, 1997.
- Van Der Mensbrugghe F., « Le service universel aux Etats-Unis », *Cahiers du Centre de recherches informatiques et droit*, n° 14, 1998.
- Van Ommeslaghe P., « L'autorégulation. Rapport de synthèse », In : *L'autorégulation*, Colloque organisé par l'ULB, Bruxelles, Bruylant, 1995.
- Vivant M., « Cybermonde : droit et droits des réseaux », *Semaine juridique*, n° 3969, 1996.
- Wilkinson A., 1998. « An Agenda for Industry Self Regulation », Discours au Mundo Internet 98, <http://www.lspo.eec.be/eif/nextgen/mundoint.html>, Madrid, 19 février 1998.
- Wittes B., « Law in cyberspace : witnessing the birth of a legal system on the net », *Legal Time*, n° 36, p. 27 et sq., 1995.